

3 1761 11648744 8

CA1
SIR
- A56

BRIDGING THE GAP

Recalibrating the Machinery of Security
Intelligence and Intelligence Review

ANNUAL REPORT 2012–2013



SECURITY INTELLIGENCE
REVIEW COMMITTEE

Canada

Security Intelligence Review Committee
P.O. Box 2430, Station D
Ottawa, ON K1P 5W5

Visit us online at www.sirc-csars.gc.ca

© Public Works and Government Services Canada 2013
Catalogue No. PS105-2013
ISSN 1921-0566

Security Intelligence
Review Committee



Comité de surveillance des activités
de renseignement de sécurité

September 30, 2013

The Honourable Steven Blaney
Minister of Public Safety
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Minister:

We are pleased to present you with the annual report of the Security Intelligence Review Committee for the fiscal year 2012–2013, as required by Section 53 of the *Canadian Security Intelligence Service Act*, for your submission to Parliament.

Sincerely,

Handwritten signature of Chuck Strahl in black ink.

Chuck Strahl, P.C.
Chair

Handwritten signature of Frances Lankin in black ink.

Frances Lankin, P.C., C.M.

Handwritten signature of Denis Losier in black ink.

Denis Losier, P.C., C.M.

Handwritten signature of Deborah Grey in black ink.

Deborah Grey, P.C., O.C.

Handwritten signature of L. Yves Fortier in black ink.

L. Yves Fortier, P.C., C.C., O.Q., Q.C.





ABOUT SIRC

The Security Intelligence Review Committee (SIRC, or the Committee) is an independent review body that reports to the Parliament of Canada on the operations of the Canadian Security Intelligence Service (CSIS, or the Service). It conducts reviews of CSIS activities, certifies the Director of CSIS's annual report to the Minister of Public Safety, and investigates complaints from the public about the Service. In doing so, SIRC provides assurance to Parliament and to all citizens of Canada that the Service investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians.

Visit SIRC online at www.sirc-csars.gc.ca for more information.



ABOUT CSIS

CSIS is responsible for investigating threats to Canada, analyzing information and producing intelligence.

To protect Canada and its citizens, CSIS advises the Government of Canada on issues and activities that are, or may pose, a threat to national security. These include terrorism, the proliferation of weapons of mass destruction, espionage and foreign-influenced activity.

It also provides security assessments of individuals to all federal departments and agencies, with the exception of the Royal Canadian Mounted Police.

A legal framework for both SIRC and CSIS

By virtue of the *CSIS Act*, Canada became one of the first democratic governments anywhere in the world to establish a legal framework for its security service. With this *Act*, Canada clearly defined in law the mandate and limits of state power to conduct security intelligence. By the same stroke, it created accountability mechanisms to keep those considerable state powers in check.

CONTENTS

MESSAGE FROM THE COMMITTEE MEMBERS	2
MESSAGE FROM THE EXECUTIVE DIRECTOR	5
ABOUT THIS REPORT	8
THE YEAR IN REVIEW	9
SUMMARIES OF SIRC REVIEWS AND COMPLAINTS	14
A. REVIEWS	14
CSIS'S Relationship and Exchanges with Communications Security Establishment Canada (CSEC)	16
Review of a New Section 21 Warrant Power	18
Investigating Activities Related to Espionage and Foreign Influence	19
CSIS Initiatives for Foreign Collection	21
CSIS's Evolving Footprint Abroad	21
CSIS'S Support to Canada's Northern Perimeter Security	23
CSIS Activities Related to Domestic Investigations and Emerging Issues	24
CSIS's Use of a Clandestine Methodology	25
The Role of CSIS in the Matter of Abousfian Abdelrazik	27
Certification of the Director of CSIS's Annual Report to the Minister of Public Safety: Overview	30
B. COMPLAINTS	33
Alleged Harassment, Racial Profiling and Sharing of Misleading Information	35
Alleged Denial of Basic Rights and Insufficient Cultural Knowledge	35
Alleged Delay in Providing a Security Assessment	36
Revocation of Security Clearances	36
SIRC AT A GLANCE	37
Committee Membership	37
Staffing And Organization	37
SIRC Activities	38
List Of SIRC Recommendations	39

MESSAGE FROM THE COMMITTEE MEMBERS

The Security Intelligence Review Committee (SIRC) exists to help ensure that security intelligence in Canada is conducted lawfully, effectively, appropriately, and with sufficient accountability. Over the past year, SIRC has engaged in, and encouraged, a process renewal and realignment in its pursuit of these key objectives. Throughout this process, the Committee has remained loyal to the duties and functions of SIRC, which has, since 1984, served as the fundamental check on the extraordinary powers granted by Parliament to the Canadian Security Intelligence Service (CSIS). Our work, summarized in this annual report to Parliament, and through it to the Canadian public, stands as our commitment to provide Canadians with as much detail as the law will allow.

SIRC's authority stems from the same legislation that created CSIS and gave that organization its role and powers: CSIS is mandated to investigate threats to national security as defined in the *CSIS Act*, while SIRC is mandated to help ensure that CSIS respects the fundamental rights and freedoms of Canadians while it does so. As an independent body reporting to Parliament, SIRC is committed to the highest level of transparency concerning our operations and the conclusions of our work, while ensuring that we maintain the strictest of standards as applied to information concerning national security. These commitments have represented SIRC's core values for almost 30 years.

Naturally, SIRC does nonetheless evolve, and this past year has seen us reach a number of significant milestones: our Committee has welcomed new Members and worked on its first products under

its newest Chair, the Honourable Chuck Strahl; we have witnessed the expansion of our mandate to include the certification of the Director of the Canadian Security Intelligence Service's annual report to the Minister of Public Safety; we have hired our first new Executive Director in over a decade; and we have taken up the challenge of reintroducing and reintegrating SIRC into the broader community of Canadian intelligence and security.

As a result, we are pleased to present nine summaries of the comprehensive reviews carried out by our agency this past fiscal year, as well as summaries of the complaints cases that were concluded during that same time frame.

When producing such a document, it is important to take a moment to recognize the individuals who helped us get to where we are today, as well as those who will bring us forward into the future. First and foremost, the Committee would like to take this opportunity to extend its most profound gratitude to former SIRC Executive Director, Susan Pollak. To say that in her 14 years of leadership, Ms. Pollak's name and that of SIRC had become interchangeable is to understate what all of us in the security and intelligence community know instinctively. Ms. Pollak shepherded SIRC and its staff through five Chairs, four CSIS Directors, the tumultuous wave of change following 9/11, two turns as host of the International Intelligence Review Agencies Conference (IIRAC), and more than 100 SIRC reviews and complaints cases. We wish her a most pleasant and serene retirement, and thank her deeply for her years of dedicated service.

On another note, the Committee would like to take the opportunity to thank former Director Richard Fadden for his years of cooperation and his cordiality. Mr. Fadden has been generous with his time and frank in his approach to SIRC over the past four years, and the Committee will look back fondly on its relationship with him as Director of CSIS. We wish Mr. Fadden success in his new position, and we look forward to working with his successor.

With an eye towards what lies ahead, the Committee would like to welcome its new Executive Director, Michael Doucet. Mr. Doucet comes to SIRC via the Communications Security Establishment, Correctional Services Canada and the RCMP, where he served as the CIO for the country's national police force. The Committee has already been impressed with Mr. Doucet's enthusiasm and leadership, as has SIRC's staff, and we look forward to the coming years of innovation and advancement under his stewardship.

SIRC has also recently welcomed Deborah Grey, P.C., O.C., to the ranks of Committee Member. Ms. Grey brings with her an incredible wealth of experience in promoting and defending the public interest on a national scale. In addition, SIRC has just welcomed L. Yves Fortier, P.C., C.C., O.Q., Q.C., as its newest Committee Member. M. Fortier's extensive background as an international arbitrator, diplomat and director of numerous Canadian corporations brings an exceedingly valued and valuable range of expertise to the Committee. It is an understatement to remark that the Chair

is pleased and excited at the prospect of drawing upon the knowledge and talent of Ms. Grey and M. Fortier over the coming years.

As predicted in the 2011–2012 annual report, the Committee spent some of its time and energy this past year taking up a new challenge, namely, guiding SIRC through an evolution of its responsibilities and mandate that saw it take on the task of certifying the CSIS Director's annual report to the Minister. SIRC was quite suited to the task of meeting this legislative requirement, and a symbiotic relationship has already begun to develop between SIRC's review function and the certification process whereby both are able to inform the other. Ultimately, it was SIRC's established expertise in the production of research reviews that facilitated this transition.

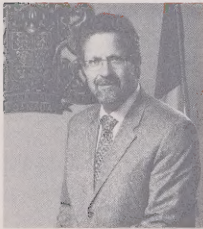
This consistency of approach between SIRC's long-standing review work and the certification process also addressed the issue of how to maintain the arm's length independence embodied in SIRC's original mandate, while simultaneously fulfilling SIRC's new legislative requirements. Since the methodology employed in SIRC's certification process is quite similar to the approach required to fulfill its other legislative responsibilities, there is no inherent conflict between SIRC's responsibility to report to Parliament and its provision of a Certificate to the Minister. Indeed, the issues identified in SIRC's certification of the 2011–2012 Director's report were addressed in recent SIRC studies and described in SIRC's 2011–2012 annual report to Parliament.

As we move forward, we also recognize the need to reinvigorate the promotion of SIRC and its staff to the wider environment of security and intelligence. Domestically, this will mean stronger ties with like review and oversight bodies, and increased consultation with the appropriate intelligence and security experts. Internationally, this will mean following up on the crucial links forged at events like IIRAC.

Finally, SIRC remains committed to promoting and enriching the critical national conversation on the aims and limits of security intelligence, and

of CSIS's duties and functions in support of those endeavours. As will be reflected in this report, which we offer with pride, we are encouraging CSIS to realign and recalibrate a range of policies and approaches to effectively and efficiently support its crucial investigative activities, thus promoting the ongoing safety and security of the Canadian public, while maintaining the freedoms and rights Canadians justifiably expect and enjoy.

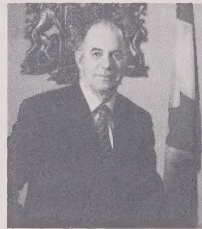
MEMBERS OF THE COMMITTEE



The Honourable
Chuck Strahl



The Honourable
Frances Lankin



The Honourable
Denis Losier



The Honourable
Deborah Grey



The Honourable
L. Yves Fortier

MESSAGE FROM THE EXECUTIVE DIRECTOR

When the Honourable Chuck Strahl appointed me as SIRC's Executive Director in December 2012, I was struck by how little was publicly known about this Committee of Privy Councillors. Having been in my new role for the better part of a year, it now seems appropriate for me to clarify what SIRC does, how it does it, and what parliamentarians and Canadians can expect of us in the future.

The Committee is composed of exceptional Canadians who leverage their previous experiences in public and private life to assess information presented to them about the activities of CSIS. Members, who are generally appointed to the Committee for five-year terms, work part-time throughout this period. As Privy Councillors, SIRC Members receive all of their information and advice about CSIS's activities from a dedicated team of full-time national security experts or through complaint hearings.

The Committee Chair delegates to the Executive Director the responsibility for the day-to-day running of SIRC. This means I am responsible for having the right people, processes and procedures in place to ensure that the Committee is adequately informed. I am additionally entrusted with ensuring the sound fiscal management of government funds provided to SIRC.

Allow me to underscore the key principles I believe are central to the work my staff and I perform on behalf of the Committee and, through them, for parliamentarians and, hence, all Canadians.

The most important principle is our independence.

The architects of the *CSIS Act* understood that SIRC had to exist as a body external to the executive branch of government to ensure that our findings and recommendations were never influenced for either bureaucratic or political reasons. The *CSIS Act* gives voice to this requirement in two complementary ways: first, SIRC employees are not members of the core public administration—the Committee functions as a separate employer. Instead, SIRC employees retain their positions at the pleasure of the Committee, meaning that their duty is to SIRC—not, for the most part, to the wider government establishment. Second, Committee Members are appointed as Privy Councillors by the Prime Minister of Canada, after consultation with the other political parties, and cannot be serving Members of Parliament. This means that although Committee Members have diverse political and regional backgrounds, they sit on SIRC in positions of trust where partisan predispositions are unwelcome.

I am well aware that one of the risks to our independence is becoming unduly influenced by the culture of secrecy, or what spy novelist John le Carré described as becoming entrapped by the “magic circle.” SIRC must therefore—and on an ongoing basis—balance the need for transparency concerning CSIS activities with the attendant requirement to protect national security information. Let me be clear: we will never jeopardize the security of Canadians by releasing information that could serve

only to buttress the Committee's image as a relevant and topical entity. Although I am confident that we always have our fingers "on the pulse" of CSIS, being responsible with the information we are entrusted with necessitates discretion.

That said, to help maintain our independence from CSIS, SIRC's main office is located in downtown Ottawa. This location also acts as "neutral" territory for the quasi-judicial process of investigating complaints, requiring that CSIS representatives come to SIRC to present their case. SIRC also has working space at CSIS headquarters; this is where SIRC staff access CSIS's corporate and operational information (hard copy and electronic formats), ranging from health services data to raw intelligence on the most classified operations. Meetings are held with CSIS employees and management, as required, including travel to CSIS regional offices and overseas stations. In short, we can gain access to whatever we need, wherever it is located. Next year, for the first time, I will be travelling to a classified foreign station; I do so as much for the information I will obtain while there as for the message it sends about SIRC's unencumbered reach.

Given this comprehensive access to national security information, I acknowledge that the confidence placed in our work is rooted in the competency of the people charged with performing the legal and research activities on behalf of the Committee.

This leads me to my second principle: maintaining a highly competent and professional workforce. As one would expect, my staff is well educated (as an example, analysts have a minimum of two post-secondary degrees). My team is composed of individuals from different academic and professional backgrounds, with many approaching, or eclipsing, 10 years of experience

in handling the most sensitive national security issues. I have spent my career in the areas of intelligence and law enforcement, having had the pleasure of working with a wide cross-section of domestic and international professionals from these fields over the past 25 years. Therefore, I can say with confidence that I am impressed by the expert assessments produced by SIRC staff. Copies of our classified reports are sent to CSIS and the Minister of Public Safety and, historically, roughly 70 percent of our recommendations are accepted by CSIS, even though they are non-binding.

As a complement to the capacity of my staff, **our third principle calls for SIRC to act as a productive and informed member of the national security community.** Although I am satisfied by the work done by my small and nimble group of experts, I am equally committed to continuously enhancing their professional capacities. As part of this, I have embarked upon a program of modernization by which additional technological and analytical systems will provide employees with updated resources to manage their legal and research processes.

In addition, I am aware that part of further evolving the expertise of my employees is through SIRC's outreach initiatives. Employees are being encouraged, whenever possible and appropriate, to liaise with academic, legal, intelligence, auditing and policing professionals. The purpose of these liaison efforts is to help ensure that SIRC staff stay well informed of issues related to their professional discipline. These exchanges also allow staff to take advantage of a large and growing body of work and experts in Canada with whom we have the privilege of consulting. This strategy serves to counteract the risk of groupthink by ensuring that employees can place CSIS's activities within the broader context in which they operate.

As I concentrate on moving forward, I am reminded that SIRC's unimpeded access to CSIS information is our *raison d'être*, and that this access has been further leveraged by incorporating certain duties previously performed by the former Office of the Inspector General of CSIS. Indeed, SIRC is now required to certify the accuracy of the CSIS Director's annual report to the Minister of Public Safety.

To ensure that my team can hone their professional understanding of CSIS to the greatest extent possible, our short- and medium-term goals involve further integrating our three core information pillars: complaints, reviews and certification.

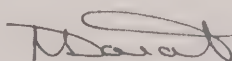
Speaking more broadly, SIRC continues to play an important role alongside Canada's intelligence community by contributing to both the classified and non-classified dialogue on national security. I envision expanding our contribution in both of those realms over my tenure as SIRC's Executive Director. This will take time and will be dependent on whether SIRC's statutory reach is expanded to pursue national security information linked to CSIS within other

federal departments and agencies. Even absent of legislative change, however, I remain confident that our efforts to evolve our work will be received by CSIS, and by Parliament, as a constructive undertaking.

In subsequent annual reports and departmental performance reports, I will continue to provide further context concerning the progress being made on advancing our capabilities in support of the Committee's mandate.

Let me state unequivocally that our independence and professionalism will never be points of compromise. We are committed to performing our duty on behalf of the Committee so that Parliament and Canadians remain confident that Canada's human intelligence spy agency is fully accountable in the performance of its duties and functions.

Sincerely,



Michael Doucet

ABOUT THIS REPORT

SIRC derives its mandate and functions from the same law that sets out the Service's legal framework: the *Canadian Security Intelligence Service Act*. In accordance with this legislation, SIRC prepares an annual report of its activities that is tabled in Parliament by the Minister of Public Safety.

This annual report summarizes SIRC's key analyses, findings and recommendations arising from its reviews and its investigations of complaints. It has three sections:

SECTION 1

The Year in Review

An analysis of key developments in security intelligence and how these relate to select findings and recommendations by SIRC from the previous year.

SECTION 2

Summaries of SIRC Reviews and Complaints

A synopsis of the reviews completed by SIRC, as well as the complaints decisions issued during the fiscal year covered by this annual report.

SECTION 3

SIRC at a Glance

Highlights the public engagement, liaison and administrative activities of SIRC. This includes details of its annual budget and expenditures.

▲ EASY ACCESS TO BACKGROUND INFORMATION WHERE AND WHEN YOU WANT IT

Look for caption boxes throughout this annual report. They contain valuable background information on various legal and policy matters related to SIRC's review and investigatory functions.



SECTION 1

THE YEAR IN REVIEW

In its 2009–2010 annual report, SIRC observed that, “periods of intense change often result in substantial policy gaps.” At that time, SIRC challenged CSIS, and Parliament, to formulate a series of questions concerning the goals and limitations of an expanded, international realm of CSIS operations and intelligence collection. In the following few years, both the Service and Parliament helped shape a framework in which those goals and limits were conveyed with greater precision—through revised intelligence priorities, more substantive guidelines on information sharing, and mechanisms to promote more effective domestic partnerships.

Having made significant strides to articulate a sharpened expression of CSIS’s current intelligence goals and priorities, the time has now come to backfill the regulations and best practices that will ensure those goals are met by employing a regime of appropriate, accountable and efficient measures. After establishing a far more directed and pronounced presence overseas, drawing upon much more vigorous and productive domestic partnerships, and reshuffling domestic priorities to foster more potent lines of collection, CSIS must now reach back into many of its programs in order to identify and align its objectives with updated policies, regulations and operational procedures.

Complementing such developments must be a commensurate shift in SIRC’s capacity to fully assess the work of the Service; since our 2010–2011 Annual Review, SIRC has put forward an argument that its current limitations in the area of review—that is, limited to CSIS’s information holdings and personnel—is falling increasingly out of step with the *modus operandi* of contemporary intelligence. Greater cooperation with domestic partners and more comprehensive regimes of information sharing mean that CSIS’s investigations now feed into and receive feedback from an increasingly large network. This theme spans the majority of reviews this year, and was evident in regard to the RCMP, DFAIT,

DND, CBSA and, in particular, CSEC. Moreover, all government departments and agencies—to say nothing of Canada's close allies—are becoming more technologically integrated. Governments across the Western world have responded and adapted, further integrating formerly separate intelligence capacities. As the technological barriers between information systems and previously stove-piped databases continue to fall, the sharing of data has become not merely possible, but routine. In the material explored in this annual report, we examine how there are both advantages and risks in this development, and we will highlight the growing challenges for their complete and effective review.

As CSIS moves to take advantage of this new capacity, SIRC must also be able to respond. It must be flexible enough to follow up and effectively review CSIS activities and investigations, even when they cross over with other agencies and departments. Given the inevitability of technological interconnectivity, SIRC must be ready with the legislative tools and matching government resource commitments to ensure that the checks and balances enshrined in the Committee remain relevant and effective.

SIRC REVIEWS

One of SIRC's largest reviews this past year delved into our ongoing interest in the increased collaboration between CSIS and Communications Security Establishment Canada (CSEC). Clearly anticipated as one of the most important intelligence partnerships of the next decade, SIRC's review highlighted both the significant potential efficiencies of closer cooperation—from shared services to filling in intelligence gaps—as well as the areas where results were not yet meeting expectations. When the focus turned to the realm of intelligence sharing, SIRC found limitations in the application of established Human Intelligence (HUMINT) procedures when applied to the Signals Intelligence (SIGINT) process; one significant risk of increased HUMINT/SIGINT collaboration is the potential erosion of control over the information shared.

Given the inevitable—and desirable—growth of cooperation between the two agencies, SIRC identified what we found to be a need to backstop many of the individual programs with a more comprehensive string of policies and procedures to address the growing volume of challenges, as well as the need to ensure that each organization continues to respect its individual and unique mandates.

In another review on a new Section 21 warrant power, SIRC similarly found that, given the current need to leverage international partnerships in order to keep track of CSIS targets when they travel outside Canada, the Service set out to maximize existing mechanisms and partnerships so as to increase its collection capacity. However, the resulting increased volume of shared information also introduced a reduced level of control over the flow—and, potentially, the use—of CSIS-originated information once it was passed off. Although this risk has already been identified by the Service in regards to one of its allies, SIRC recommended that the use of “caveats”—articulated limits and conditions on the use of CSIS information—be extended to a wider range of international partners.

SHORING UP LIMITS AND THRESHOLDS

As both SIRC and CSIS have been stating for several years, while counter-terrorism remains one of the highest intelligence priorities, counter-espionage has returned to the forefront of intelligence work. Echoing levels last seen during the Cold War, CSIS's long-standing role to advise government of threats emanating from state-sponsored offensive intelligence efforts has evolved from more straightforward “classic” counter-intelligence strategies and activities (e.g. political and military), to gathering information on commercial and financial data, following webs of influence and, perhaps most formidably, parcelling out terabytes of information to identify the occurrence and origin of foreign-sponsored attacks in the cyber realm. SIRC found that one of the foremost challenges of collecting and analyzing espionage-based information is, as it has often been, sorting out the “legitimate”

efforts of another state acting within Canada from the “clandestine” range of activities.

Given the seemingly endless range of platforms and techniques within which espionage can now take place, the challenge CSIS faces in remaining within the boundaries of the “strictly necessary” limitations of the powers accorded to them in the *CSIS Act* is significant. As a result, SIRC recommended that CSIS fine-tune its existing policy and practice in this area to assist investigators in identifying common and consistent thresholds, and create firmer indicators and tools to help define when an activity has crossed over into the clandestine realm.

Another SIRC review examined some of the initiatives now underway to support CSIS’s foreign collection programs. Having now firmly established the need and mandate for such collection, CSIS has moved into a phase of evaluating and improving the tools and policies that underscore and establish its capacity to do so. SIRC was satisfied with what it perceived was a consistent and constant message throughout the branches of the Service that maintained that foreign collection is always firmly anchored to a Canadian nexus, and that such collection is never allowed to take priority over domestic investigations. However, given the increased challenges—operational and legal—of operating outside Canada’s borders, SIRC did find that CSIS had gaps to fill, both in regards to the availability of training (particularly for individuals deployed to dangerous environments), and in regards to the legal limitations of intelligence options. As CSIS’s overseas operations bring the Service into new scenarios, the opportunities they represent—and the potential risks they carry—are going to require CSIS to develop a more comprehensive legal framework that will clearly delineate what kinds of activities will be acceptable, and which will be prohibited.

In an additional review—SIRC’s annual foreign post review—we took the view that CSIS’s operations abroad are not expanding as much as they are evolving. The ongoing restrained fiscal environment has meant that CSIS cannot pursue with equal vigour

every potential operational lead to which it is privy overseas (and there are many), but must decide which leads to explore, and to what extent. Again, having received government direction and having established guidelines on information sharing with both trusted allies and agencies suspected of human rights violations, CSIS must now fill in the procedural gaps that present themselves when such arrangements begin to produce intelligence. In some instances, such expectations have been met, while in other instances, SIRC found that some specific tools CSIS utilizes to inform its own decision-making were somewhat deficient.

INSTITUTIONALIZING RESPONSIBILITY

As a final kind of “gap” that emerged as SIRC examined the reshuffling of priorities and investigations, the need to establish a firm and consistent chain of responsibility was noted in several reviews. One such review, which centered on CSIS’s support to Canada’s Northern Perimeter Security, noted how the issue shifted over the past few years, given the need to strike a balance between the government’s emphasis on the Arctic as a prescient security concern, and the historic dearth of intelligence collection in that region. Ultimately, SIRC found that despite some gained efficiencies, CSIS’s northern strategy was still too dependent on a mix of serendipity and the personal engagement of a string of internal Service champions. Over the long term, CSIS, which under centralized rather than regionalized leadership, will have to develop a concentrated strategy that hammers out a concrete, multi-year strategy, backed up by the appropriate resources.

On the other side of the coin, SIRC examined CSIS activities related to domestic investigations and emerging issues. Over the past few years, long-standing domestic concerns such as environmental extremism, white supremacy, and secessionist extremism, have, to varying degrees, faded from view. As a result, CSIS reassessed and retooled those investigations to draw down on areas that were showing few signs of active threat, while at the same time re-imagining the categorization of extremist ideologies (left, right, etc.) so as to

be less concerned with the philosophical orientation but as concerned with the potential for violence. The result was the efficient termination of reporting and investigation of some long-standing but increasingly inactive targets. The remaining risk involves the possibility of a sudden flare-up of domestic violence, prompting an immediate request on the part of government for information. To help mitigate that risk, SIRC noted and encouraged CSIS's strategy of maintaining active liaison with its domestic partners—especially in law enforcement—who maintain an awareness of the same groups due to their spill over into criminal behaviour.

The last example reviewing the institutionalization of responsibility emerges from SIRC's first production of the certification of the CSIS Director's annual report to the Minister of Public Safety. Overall, SIRC emerged from this intense exercise largely satisfied with the quality and completeness that characterized the Director's report. However, when it came to describing CSIS's overseas operations, SIRC found that the quantity and detail of what was included in the report was not as comprehensive as it could have been. Given that the object of that section would be to provide the Minister with a strong understanding of the increasingly elevated threats to the lives of Service employees and its operations overseas, SIRC noted that more detailed information would provide a more accurate and representative description of CSIS activities. SIRC noted that the Director of CSIS may wish to include more information in this area next year, and that the issue is of sufficient concern to warrant the Minister's attention and continued consideration.

WRAPPING UP COMPLAINTS

This year also saw the completion of five complaints cases; as with SIRC's reviews, the recommendations stemming from these cases concerned the filling of gaps and an increased measure of standardization across CSIS practices. For example, in the case of one complaint surrounding the immigration interview process, SIRC recommended that CSIS

adopt the practice of one region—to consistently prepare and test the recording devices prior to such interviews—and apply it to all regions of the Service. In a separate case, SIRC noted that some government employees require, from time to time, a review of the instances and conditions under which they can and cannot divulge the identity of their employer.

COMING FULL CIRCLE: THE CASE OF ABOUSFIAN ABDELRAZIK

The past year also witnessed the completion of SIRC's review of CSIS's role in the matter of Abousifian Abdelrazik. In that review, SIRC concluded there was no indication that CSIS requested Sudanese authorities to arrest or detain Abdelrazik, but found that CSIS kept its allies informed of fresh intelligence concerning his case once he departed Canada. Moreover, SIRC found that the two Canadian government organizations most heavily involved in this case carried out their respective consular and intelligence work concurrently—sometimes at odds—with each other. SIRC also raised concerns surrounding: the inappropriate disclosure of classified information; the creation of an intelligence assessment that exaggerated and inaccurately conveyed information to Government of Canada's partners; and the excessive reporting in operational databases of information not related to the threat, originating from individuals who were not targets.

However, given that it has been a decade since the events described in much of SIRC's report took place, the remedies and recommendations that would adequately address SIRC's concerns have already been covered in previous SIRC reports, as well as other venues such as Commissions of Inquiry. Although SIRC encouraged CSIS to use this review as an opportunity to revisit the applicable range of SIRC recommendations provided over the last decade, we did not provide any novel (and likely duplicative) recommendations.

THEN AND NOW

In regards to the broader themes identified in the rest of SIRC's reviews discussed above, it is interesting to note a contrast. The review of the case of Abousfian Abdelrazik centred on CSIS's activities in the first half the 2000s, a period in which most of the guidelines and decisions concerning overseas operations were yet to be made. As SIRC emphasized in that review, it should be unsurprising that SIRC did not make any new recommendations in that case, given that a combination of CSIS policy shifts and previous SIRC recommendations had already addressed the concerns raised by the review. In the early and mid-2000s, CSIS, the government and the Canadian public were still wrestling with questions concerning whether CSIS's activities should expand overseas, the extent to which that expansion should occur and what it meant for both the Service and the Canadian intelligence community as a whole.

In 2013, that debate has moved to the next stage. The discussion now turns to how best that job should be done, what gaps remain in CSIS policy and procedure to operate in the current security intelligence environment, and what measures remain in place and are enforced to ensure the continued exercise of the Service's powers within the limitations of its mandate.

SECTION 2

SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

A. REVIEWS

SIRC's reviews are designed to provide Parliament and the Canadian public with a broad understanding of the Service's operational activities. In carrying out its reviews, SIRC examines how CSIS has performed its duties and functions to determine retrospectively if the Service was acting appropriately, effectively and in accordance with the law.

WHAT IS THE DIFFERENCE BETWEEN AN OVERSIGHT AND REVIEW BODY?

An oversight body looks on a continual basis at what is taking place inside an intelligence service and has the mandate to evaluate and guide current actions in "real time." SIRC is a review body, so, unlike an oversight agency, it can make a full assessment of CSIS's past performance without being compromised by any involvement in its immediate, day-to-day operational decisions and activities.

HOW REVIEWS ARE CONDUCTED

SIRC's reviews provide a retrospective examination and assessment of specific CSIS investigations and activities. The Committee's research program is designed to address a broad range of subjects on a timely and topical basis.

In deciding which matters to review, SIRC considers:

- events or developments with the potential to represent threats to the security of Canada;
- intelligence priorities identified by the Government of Canada;
- activities by CSIS that could have an impact on individual rights and freedoms;

- ▀ issues identified in the course of SIRC's complaints functions;
- ▀ new directions and initiatives announced by or affecting CSIS; and
- ▀ the CSIS Director's classified annual report, which is submitted to the Minister of Public Safety.

Each review results in a snapshot of the Service's actions in a specific case. This approach allows SIRC to manage the risk inherent in being able to review only a small number of CSIS activities in any given year.

SIRC's researchers consult multiple information sources to examine specific aspects of the Service's work. As part of this process, researchers may arrange briefings with CSIS employees, as well as examine individual and group targeting files, human source files, intelligence assessments and warrant documents.

SIRC can also examine files relating to CSIS's cooperation and operational exchanges with foreign and domestic agencies and partners, among other sources, that may be review-specific. The goal is to look at a diverse pool of information so that we can ensure we have thoroughly reviewed and completely understood the issues at hand.

FIND OUT MORE ABOUT SIRC'S EARLIER REVIEWS

Over the years, SIRC has reviewed a wide range of CSIS activities. A complete listing of the Committee's past reviews can be found on SIRC's website (www.sirc-csars.gc.ca).

The Committee's reviews include findings and, where appropriate, recommendations. These reviews are forwarded to the Director of CSIS and Public Safety Canada.

ACCOUNTABILITY MATTERS

SIRC is one of several mechanisms designed to ensure CSIS's accountability. The Service also remains accountable for its operations through other mechanisms such as the Minister of Public Safety, the courts, the central agencies of government (i.e. Privy Council Office, Treasury Board Secretariat), the Auditor General of Canada, the Information Commissioner of Canada and the Privacy Commissioner of Canada.

TRACKING SIRC'S RECOMMENDATIONS

Each year, SIRC requests a status report from CSIS on the recommendations arising from the previous year's reviews and complaint decisions. This update gives SIRC the opportunity to track the implementation of its recommendations and to learn about the practical impact of those recommendations on CSIS.

This process also allows CSIS to respond formally to SIRC's reviews and decisions, and forms part of the ongoing dialogue between the two organizations. During the 2011–2012 review period, SIRC made nine recommendations addressing a wide range of issues.

SIRC is pleased to note that CSIS has responded to several of these recommendations. For example, CSIS agreed with SIRC's 2011–2012 recommendation to revise the Service's policy on caveats so as to reflect current information-sharing practices and processes with foreign partners.

SIRC REVIEW

CSIS'S RELATIONSHIP AND EXCHANGES WITH COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

Background

The government's decision to locate CSEC headquarters alongside CSIS headquarters is illustrative of a global trend in which the once-solitary worlds of Human Intelligence (HUMINT) and Signals Intelligence (SIGINT) have increasingly merged. This trend has been driven by expanded demands from the government for timely and relevant information, to maximize operational efficiency in an age of fiscal restraint, and to address an evolving and increasingly technologically complex global threat environment.

This review explored the benefits to CSIS from increased cooperation with CSEC, both through an examination of operational and non-operational initiatives. The review examined combined efforts at coordinating corporate services, ensuring sufficient inter-organizational knowledge transfer, how operational risks are managed, the collection of non-threat-related information (cf. *CSIS Act*, Section 16), and the adequacy of direction and policies used to help guide CSIS's information sharing with CSEC.

SIRC's Review

The review found that a number of challenges prevent CSIS and CSEC from fully capitalizing on the opportunities presented by the new proximity of their respective headquarters. For intelligence agencies

faced with increasingly limited resources, shared services allow for efficient and effective resource management. Unfortunately, SIRC found that the initial expectations for shared services between CSEC and CSIS may have been too optimistic.

Although the new CSEC facility has not yet been completed—leaving open the possibility for greater-than-expected returns—to a significant extent, the potential efficiencies have thus far been offset by managerial issues, budgetary restrictions and complications related to CSEC site development.

More generally, SIRC found that CSIS and CSEC had gaps in understanding the other organization's respective mandate and/or responsibilities. This impediment to cooperation was raised at both the working and managerial levels across CSIS's operational branches, and acknowledged at joint CSIS/CSEC meetings. Moreover, these gaps in understanding resulted in instances where CSIS policies or procedures were not followed, an outcome that could have negatively impacted operational risk.

For its part, CSIS acknowledged the challenges associated with overlapping mandates and, quite often, the unique demands of the overlapping activities involved in the deployment or use of sensitive CSEC technology or CSIS human sources. Solutions presented to SIRC to address these problems include further educating CSEC and CSIS operational desks on relevant policies, as well as the creation of a joint CSIS and CSEC senior management operational board to provide strategic-level management on these activities.

FOREIGN INTELLIGENCE COLLECTION

Section 16 of the *CSIS Act* defines foreign intelligence as any information about the capabilities, intentions or activities of a foreign state, foreign national or foreign organization (i.e. non-threat-related information). By contrast, Section 12 of the *CSIS Act* defines security intelligence as information and intelligence related to "threats to the security of Canada." Despite considerable cooperation with CSEC on foreign intelligence collection activities within Canada, there remained some internal debate within the Service about the extent to which these activities negatively impact CSIS's primary mandate to collect security intelligence. As a result of the varying accounts provided by CSIS on this issue, SIRC cautioned the Service to be prudent when deciding the extent to which it continues to seek CSEC's assistance in the Section 16 process. Unless changes to the *CSIS Act* are made, CSEC, not CSIS, remains the organization primarily mandated with providing the Government of Canada with foreign intelligence information.

Information Sharing

The above notwithstanding, a large proportion of the review was focused on how CSIS and CSEC share information. Normally, whenever CSIS shares information, it uses caveats and/or assurances. Caveats stipulate that the information being provided is CSIS property and cannot be forwarded to another agency or altered without CSIS's direct consent. Assurances are formal, bilateral agreements made with foreign agencies stipulating that CSIS's information will not be used in a manner that runs contrary to international human rights conventions. The extent to which caveats and assurances are effective depends on the degree of trust between CSIS and the agency receiving the information. SIRC found, however, that a significant risk of increased HUMINT to SIGINT collaboration is the potential erosion of control over the information shared.

The Committee reached this conclusion because CSIS's caveats and assurances were never designed for SIGINT collection. Unlike HUMINT agency collection, which is often done in isolation (i.e. collecting information from a human source and, if desired, subsequently sharing that information with an allied agency), SIGINT collection is instead more of a collective undertaking. CSEC belongs to a special alliance that includes the United States National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Defence Signals Directorate, and the New Zealand Government Communications Security Bureau. The CSEC Commissioner's Office, in its 2011–2012 annual report, described these partnerships as being potentially "more valuable now than at any other time, in the context of increasingly complex technological challenges."

For its part, CSIS believes that exchanges with CSEC are low-risk endeavours. This is premised on the fact that allied SIGINT agencies, irrespective of the broad sharing that transpires among them, are primarily focused on their own national intelligence priorities. However, of concern to SIRC are those instances when allied collection priorities have coalesced with Canada's—such as in counter-terrorism cases.

Although ministerial direction to CSIS and associated Service policies are designed to prevent the misuse/abuse of information, both from a security and human rights perspective, it is not clear how CSIS can comply with ministerial direction stipulating that caveats must be used when sharing information with domestic and foreign recipients, when SIGINT collection and dissemination functions run contrary to this expectation.

CSIS has acknowledged to SIRC that addressing these concerns is a complex subject that remains a work in progress; considering that the collaboration between CSIS and CSEC is increasing, SIRC will revisit this issue in subsequent reviews in order to assess what progress has been made in addressing this challenge.

A Final Issue: Cyber Security

The final section of the review identified an anomaly of the CSIS/CSEC relationship, namely, a noted lack of cooperation on cyber security. In 2010, Public Safety Canada created a whole-of-government strategy, the Cyber Security Strategy, which asserts that there can be no ambiguity in terms of who does what. The Strategy confirms the respective roles of CSEC and CSIS: the former has the recognized expertise in dealing with cyber threats and attacks, while the latter is broadly tasked to analyze and investigate domestic and international threats. The Strategy notwithstanding, SIRC's review found that there is still work to be done to coordinate CSIS's cyber-related activities with CSEC, especially with respect to the protection of information and infrastructures of importance to the Government of Canada.

Given the inevitability of growth in CSIS/CSEC collaboration, **SIRC recommends that CSIS develop clearer and more robust overarching principles of cooperation with CSEC. These principles should address the growing volume of challenges that have arisen between the two bodies, while respecting the individual mandates of each organization.**

SIRC REVIEW

REVIEW OF A NEW SECTION 21 WARRANT POWER

Background

This review was SIRC's first examination of a new warrant power under Section 21 of the *CSIS Act*, which was initially authorized by the Federal Court in 2009. This new power was introduced in order for the Service to maintain coverage of targets who represented a threat to Canada as they travelled or, in some cases, resided, overseas. The review examined the processes, policies and controls that CSIS has put in place to manage the new power, as well as CSIS's cooperation and exchanges with domestic partners. The review also sought to evaluate how important the information obtained from this power has been to the Service's investigations thus far.

SIRC's Review

During the review period, 35 warrants (plus seven supplemental warrants) that included the new power were issued. The Committee found that CSIS encountered several challenges, including the efficacy of collection; control of the information collected; and possibly unrealistic future expectations. Indeed, it was noted that by relying on partner agencies—both domestic and foreign—for collection, some efficiency will ultimately be sacrificed. There has

been substantial progress since the first warrant was issued; however, CSIS is still in a learning phase and it will need to manage expectations against the realities, meaning limitations, of reporting from this collection.

In order to maximize collection under the new warrant power, CSIS, in almost every case, leverages the assets of the Five Eyes community (Canada, plus the United States, the United Kingdom, Australia and New Zealand). SIRC noted that even with the assistance of allies, the collection or intelligence yield under this power has provided different gains and challenges than the Service initially expected.

The arrangements with partners and allies also present possibilities for other agencies to act independently on CSIS-generated information. In practice, if an allied agency were to pick up intelligence on a Canadian citizen, a Canadian agency would ideally take the lead based on an informal agreement governing interactions amongst the Five Eyes partners. Nonetheless, it is understood that each allied nation reserves the right to act in its own national interest. National security legislation in both the United States and the United Kingdom, for example, gives these countries the authority to retain and act on intelligence if it relates to their national security, even if it has been collected on behalf of another country, such as Canada.

WARRANTS

	2010–11	2011–12	2012–13
New warrants	55	50	71
Replaced or supplemental	176	156	165
Total	231	206	236

The risk to CSIS, then, is the ability of a Five Eyes partner to act independently on CSIS-originated information. This, in turn, carries the possible risk of detention or harm of a target based on information that originated with CSIS. SIRC found that while there are clear advantages to leveraging second-party assets in the execution of this new warrant power—and, indeed, this is essential for the process to be effective—there are also clear hazards, including the lack of control over the intelligence once it has been shared.

Conclusions

SIRC has seen indications that the Service has started using caveats that require allied agencies to contact CSIS in the event that information based on Service information is to be acted upon. The caveats, as they currently stand, are still considered a “work in progress” by the Service, but they do not yet address the wider reality of this type of collection. Nonetheless, they are a useful tool and do provide some measure of CSIS coverage. This coverage, however, comes with several challenges, including control of the information CSIS seeks to collect. SIRC advised CSIS to devise appropriate protections for the sharing of Service information, and to keep itself as informed as possible concerning the potential uses of CSIS information.

Moreover, for the most part, these caveats, as part of the wider “assurances” regime, were only considered with regard to one partner. **Therefore, SIRC recommends that CSIS extend the use of caveats and assurances in regards to this new warrant power to include the agencies of the entire Five Eyes community, in order to ensure that no dissemination occurs without the Service’s knowledge.**

SIRC REVIEW

INVESTIGATING ACTIVITIES RELATED TO ESPIONAGE AND FOREIGN INFLUENCE

Background

Countering terrorist threats continues to be the number one priority for CSIS; however, Canada has been experiencing levels of espionage comparable to the height of the Cold War and nations involved in such state-sponsored activities are changing their tactics. In response, CSIS’s primary role is to advise Government of Canada departments to better

understand the emerging threats linked to newer forms of espionage and counter-intelligence, thereby maintaining an awareness of the foreign policy, trade and intelligence interests of specific nations.

SIRC’s Review

This study reviewed how CSIS is dealing with the rapidly changing threat posed by espionage and foreign-influenced activities. From CSIS’s perspective, the new challenges and complexities of investigating such activities are also seen as opportunities to look beyond traditional forms of espionage and delve into new operational domains. SIRC focused on CSIS’s provision of advice when dealing with different forms of foreign-influenced activities.

Within Canada there exists a long history of diplomats, intelligence officers and foreign national business leaders conducting covert activities in order to advance the interests of their respective countries. Such foreign-influenced activities become more serious when high-ranking Canadian officials or prominent members of the business community are strategically targeted. Although some of the strategic relationships pursued by foreign national representatives are mere extensions of diplomacy, the activities are considered to be threat-related and of interest to CSIS when they covertly try to obtain information or to influence decision-making.

One of the challenges for CSIS is continuing to make the distinction between what is considered clandestine and what is legitimate diplomacy. In the past, detecting covert forms of foreign influence may have been more straightforward, since much of the activity was done through traditional approaches, and foreign agents of influence were usually the focus of CSIS investigations. However, methods used by foreign actors are continuously evolving.

In the cases of foreign-influenced activities examined for this study, the negative elements are clear: democratic principles are being challenged and direction is coming from a foreign government; however, the clandestine elements are not so apparent. From the Committee’s perspective, a number of the activities being investigated appear to be more overt than clandestine. SIRC noted that although activities by foreign states may be organized and focused, such approaches are not, in and of themselves, indicators of secret activity.

As investigations into espionage and foreign-influenced activities continues to grow in size and complexity, so too will the challenge of distinguishing between what is clandestine and what is legitimate. SIRC believes that clarifying this distinction is important, since collecting information on threat-related issues must, according to the *CSIS Act*, be “strictly necessary.” **SIRC recommends that CSIS carry out the appropriate fine-tuning, in policy and practice, to assist investigators and analysts in identifying common and consistent thresholds, and in judging when an activity has crossed over into the clandestine realm.**

Adjusting the Approach

In recent years, agents of foreign interference have been targeting individuals and groups within smaller subsections of Canadian society in order to leverage those relationships into greater domestic influence. To take one example, some foreign elements have attempted to reach out to some subsections in an attempt to potentially bypass other jurisdictions, such as federal, provincial or municipal governments. CSIS will often alert affected parties (e.g. politicians, corporate executives, academics and other influential individuals) by providing security briefings and advice; however, such measures are not afforded to all affected communities.

CSIS is using this “wait and see” approach for several reasons: in addition to not having enough specific information on the potential targets or the intended offensive strategy, the Service is also concerned about how its message—any message—may be received by some communities, and whether those messages will be viewed as a positive. SIRC recognizes the Service’s concerns; nonetheless, not informing all Canadian communities about the security issues around a particular threat, while informing other sectors of society, is problematic. By trying to gather information on foreign-influenced activities without informing all communities, CSIS could actually increase distrust, especially if these communities

become informed of CSIS activities through other channels. As such, **SIRC recommends that CSIS develop a strategy to deliver the same cautionary messages about foreign-influenced activities for all potentially affected sectors.**

A Growing Concern

In recent years, the potential risks to national security from state-owned enterprises (SOEs) originating from foreign countries has been of increasing interest to the Government of Canada. CSIS informed SIRC that advice to the Government of Canada that touches on SOEs is not aimed at stopping investment; rather the Service provides information so that the government can make a fully informed decision on trade and relations with foreign partners. CSIS also participates in the *Investment Canada Act* (ICA) process. In 2009, the *National Security Review of Investments Regulations* provisions within the ICA were registered and became a new business line for CSIS. One purpose of the ICA is to review significant investments in Canada by non-Canadian entities. Despite the short timelines within which this activity takes place, CSIS is an important part of the larger process whereby the Minister of Public Safety assists the Minister of Industry in determining whether the proposed investment could or would be injurious.

Canada’s recent foreign policies and international trade agreements will likely result in greater client demands for information on SOEs, and other economic/prosperity issues. SIRC will monitor the evolution of CSIS’s involvement in such processes with interest in the years to come.

On this file overall, SIRC found that CSIS has acted appropriately under current operational policies; however, some adjustment may be required as new strategies by foreign nations emerge. SIRC will be interested to see how CSIS’s investigation into threats posed by espionage and foreign-influenced activities of foreign governments develops in the future.

SIRC REVIEW

CSIS INITIATIVES FOR FOREIGN COLLECTION

Background

CSIS Director Richard Fadden noted in February 2013 that the Service is “aware of dozens of Canadians” who have travelled or attempted to travel to engage in terrorist activities. CSIS is hoping that foreign collection initiatives will help to close this information gap. Indeed, SIRC has also seen how ministerial direction and emerging issues such as kidnappings and illegal migration have placed demands on the Service to report on overseas activities. Foreign collection operations help CSIS identify threats before they reach Canada. They also help decrease the Service’s dependence on allied reporting, focusing collection efforts on Canadian-related foreign-based threats.

SIRC’s Review

This review centred on efforts by two branches to enhance their overseas intelligence collection abilities. The review continued SIRC’s ongoing examination of how CSIS is operating abroad with partner intelligence services, while also independently working to fill information gaps. Both branches worked with the various CSIS regional offices to create frameworks for the intelligence collection priorities, methods and goals of overseas collection, and to connect them back to Canadian concerns. The documents outlining such initiatives are frequently updated to reflect the ongoing evolution of the threat, or changes with regard to intelligence gaps.

In March 2012, the Service created a dedicated unit to provide training related to operations, in part because CSIS recognized that it was increasingly venturing into more dangerous areas. Training modules are tailored to the individual operation and include a feedback mechanism. Incorporating such a mechanism as a routine task is an excellent method of ensuring a better product; SIRC found that the lessons learned and the iterative approach adopted in the development of the training modules to be good practice.

An important benefit of having these training modules is that it allows CSIS to take an ongoing critical look at any operational shortcomings. The training and

evaluation can also provide a measure of objectivity and help mitigate any differences of opinion when it comes to deciding to operate in a potentially dangerous environment. **SIRC supports the development of operational training and recommends that the Service ensure that all persons who are identified as a priority for training receive it, particularly if they are operating in a dangerous environment.**

Overall, SIRC found that CSIS is taking a measured and cautious approach with the initiatives examined in this review. Safety continued to be a paramount consideration and was mentioned at all of SIRC’s briefings; SIRC saw no indication that people would be brought into any new initiative if it was felt they would be in jeopardy or would not meet with some measure of success. SIRC was also reassured to find a consistent message highlighting the fact that the primary focus of the regional offices and collection programs was always domestic collection, and that such collection is never to be sacrificed in order to collect abroad. With regard to overseas activities, **SIRC recommends that CSIS develop a legal framework outlining acceptable and prohibited activities, including the corresponding levels of approval within and outside the Service.**

SIRC REVIEW

CSIS’S EVOLVING FOOTPRINT ABROAD

Background

CSIS foreign stations are strategically located in order to meet Government of Canada intelligence needs, which include: the provision of security screening support to Citizenship and Immigration Canada offices abroad, liaising with other partners (both international and domestic) located abroad, and collecting intelligence on possible threats to Canada or Canadian interests. With the exception of Paris, Washington and London, and CSIS’s presence in Afghanistan, the location of foreign stations remains classified. Typically, past SIRC reviews have examined liaison efforts and operational activities within a single station abroad. This year, SIRC took a broader focus and looked at CSIS’s overseas presence writ large, focusing on the decision-making surrounding the Service’s overall approach to its representation abroad.

SIRC's Review

This review was guided by some key items, including: the criteria for opening and closing stations, the challenges of operating overseas, and the assessment of arrangements with foreign agencies. Overall, SIRC found that CSIS, in attempting to broaden its operational role overseas, is being strategic and capitalizing on both its liaison and operational functions. Nonetheless, SIRC outlined a few noteworthy issues concerning: the accuracy of information provided in some of its foreign arrangement profiles; how priorities are determined when collecting on specific intelligence requirements abroad; and the implications surrounding the long-term sustainability of playing a more operational versus a liaison-centric role.

The broader question of whether CSIS is being asked to do more with less was not a question that could be answered within this review. Rather, SIRC notes that CSIS's footprint abroad is evolving rather than merely expanding, and that the requirements of the Government of Canada, including fiscal restraint, have encouraged a more dynamic approach to this evolution. New strategies are in place, which CSIS hopes will provide the flexibility required to respond to its ongoing collection requirements, as well as any emerging issues that may arise and require attention.

However, there are other challenges associated with stepping into rich areas of collection, and SIRC outlined that existing opportunities do not completely counter them. For instance, the staff in one of the stations examined found challenges in managing the competing demands that CSIS faces in relation to not only day-to-day administrative duties, but key liaison functions and complex operational activities. This underscores some of the differences that exist between liaison-centric posts and the more operational posts located in other parts of the world.

An evolving operational presence abroad has also meant a changing dynamic of how CSIS is dealing with foreign intelligence agencies. This has translated into the enhancement of existing arrangements, the re-activation of suspended or dormant relationships, and the pursuit of new partnerships. The requirement to work and deal with a limited pool of potentially

problematic partners in certain parts of the world is inevitable, and poses additional challenges. This reality is nonetheless juxtaposed with reasonable questioning and research on the questionable track record of some of these agencies and its personnel.

As per Section 17 of the *CSIS Act*, the Service may enter into arrangements with foreign entities. Another illustrated challenge, both in terms of liaison and conducting operations abroad, is the possible corruption within some of these agencies. In one arrangement profile that SIRC examined, previous concerns with respect to corruption had led to temporarily suspending this relationship. In an attempt to revive this arrangement to meet some operational requirements, corruption issues were still deemed to be a potential concern; however, CSIS relied on an incremental risk-based approach. SIRC found that prior to the Service re-engaging with the foreign agency, CSIS took appropriate steps to assess current corruption concerns.

Information related to foreign arrangements is contained in the *CSIS Act*, Section 17 "Arrangement Profile." These arrangement profiles are used to brief the Director, the executive, the branches and regional offices, as well as external departments and entities, including SIRC. As such, the accuracy and relevancy of such profiles is of utmost importance. SIRC found some deficiencies regarding content within three arrangement profiles it examined. SIRC also found that in at least one case, critical information contained in a source file was not used to keep an arrangement profile accurate and up-to-date.

SIRC has commented in the past on the accuracy and maintenance of Section 17 profiles and further found that although progresses have been made with regards to regular updates, there is still a need for significant improvements, particularly in regards to populating the content of the documents. As SIRC was informed throughout this review, operations abroad are no longer the exception but now the norm. As such, accurate and up-to-date information on foreign agencies is crucial not only to the success of the operation, but also to maintaining positive liaison relationships.

As overseas operations expand and evolve, the accuracy of information contained within these arrangement profiles becomes more important than ever. As such, **SIRC recommends that CSIS take immediate action to ensure that Section 17 profiles are consistently accurate, complete, up-to-date and relevant.**

SIRC REVIEW

CSIS'S SUPPORT TO CANADA'S NORTHERN PERIMETER SECURITY

Background

Canada's North is undergoing rapid transformation: from the impacts of climate change, to advances in oil, gas and mineral exploration and development, as well as the growth of northern and Aboriginal governments and institutions. Not all of the interest in this vast region, however, is benign: national security concerns in the North—long perceived as a bygone threat of the Cold War—are once again receiving media, academic and government attention.

Each of the eight circumpolar states (i.e. Canada, Finland, Greenland [Denmark], Iceland, Norway, Russia, Sweden and the United States) has its own definition of what constitutes the circumpolar region, the Arctic, and the North. Canada tends to differentiate between the “near north” and the “far north.” The near north is typically defined as constituting the landmass between 50° and 60° latitude, while the far north is generally regarded as encompassing all areas north of 60° latitude (i.e. the Arctic). These distinctions are important for CSIS, as there are different liaison, operational and financial considerations between operating in the near north versus the far north of Canada.

SIRC's Review

Advancing the government's northern interests has become a priority in recent years; as such, this study focused on the rationale(s) underscoring CSIS's efforts at securing Canada's northern perimeter. In particular, the study examined the extent of the threat(s) as understood by the Service, how resources devoted to this issue are managed (at headquarters and within CSIS's

regional offices), CSIS's liaison activities with relative northern partners, and how operational initiatives have been developed and acted upon.

In particular, SIRC found that CSIS faced a number of unforeseen challenges following the government's decision in 2010 to designate the Arctic as an intelligence and security “issue” in its own right. To begin, the Service had traditionally not played a significant role in working collaboratively with relevant stakeholders on northern issues. Absent a dedicated “Arctic portfolio,” what resources that were expended on the subject were devoted to investigating what had historically been a limited number of threats. Therefore, CSIS was forced to confront a topic that had hitherto been viewed as a fairly low priority.

Despite being encouraged by the government to realign its resources alongside this northern-focused priority, SIRC found that CSIS's efforts at addressing this direction were difficult to implement due to an additional government priority calling for fiscal restraint. The problem with the resulting curtailment in resources is that it occurred precisely when CSIS was trying to reassess the relative importance of threats in the North, their complexity, and how resources should be focused for targeting and source recruitment.

In 2011, CSIS received new and more specific direction on what was expected vis-à-vis Canada's North. This was followed by an internal reorganization of responsibilities within the Service aimed at increasing the efficiency and effectiveness of resources devoted to this subject. SIRC found that as a result of this new direction and regional reorganization, CSIS's strategic management of the northern question became more consistent with the approach taken for other regional responsibilities.

Despite the directional and the resulting organizational changes, challenges remain. First, there is the larger and general prevalence of a pervasive (“southern”) attitude of indifference towards Canada's North that must be overcome each time investigative considerations (or the subsequent request for associated funding) is discussed; second, there are pressing operational priorities in Canada's south (and overseas)

that take up the lion's share of CSIS's resources; and, finally, there are continuing financial pressures limiting operational options. Added to this is the absence of an official CSIS headquarters strategy guiding the Service's northern efforts; instead, there is a reliance on shared regional responsibilities, which can complicate the prioritization of northern initiatives.

Although SIRC found there was general agreement among CSIS managers that the *status quo* was satisfactory, looking over the longer term (i.e. five years and more), some senior officials believed that a stronger role by CSIS headquarters would become necessary. SIRC agrees; one initial initiative would be for CSIS to conduct an internal study on establishing a long-term operational strategy for Canada's North, paralleling sound efforts undertaken prior to the Service's expansion overseas. Such an approach would be consistent with the importance the government places on this issue and, further, would better position the Service to react to national security requirements when (not "if") they become more prominent within Canada's northern frontier.

Regardless of the specific manner in which it is implemented, however, **SIRC recommends that CSIS "institutionalize responsibility" for northern initiatives by setting out headquarters-driven liaison and operational objectives over a multi-year period, and ensure that these objectives are sustained with an appropriate resource commitment.**

SIRC REVIEW

CSIS ACTIVITIES RELATED TO DOMESTIC INVESTIGATIONS AND EMERGING ISSUES

Background

CSIS characterizes domestic extremism as the willingness of individuals or groups in Canada to use violence or the threat of violence for political and/or ideological purposes. While CSIS dedicates most of its counter-terrorism resources to religious extremism, the Service also continues to monitor individuals and organizations that might be involved in other forms of terrorism, including violence related to issues such as: animal rights, the environment, anti-globalization

and white supremacy. Violence associated with these domestic themes tends to fluctuate and often revolves around events or current issues; moreover, the vast majority of activities related to these issues or events falls well within the realm of legitimate protest. In recent years, the level of threat associated with a number of such domestic investigations has been reassessed, particularly in light of the conclusion of key, large-scale events in 2010 (e.g. the Vancouver Olympics and Paralympics, and the G8 and G20 summits) that may have temporarily attracted violence, or the increased threat of violence. Accordingly, CSIS has made changes to the ways it investigates non-religious domestic extremism in the wake of this threat reassessment.

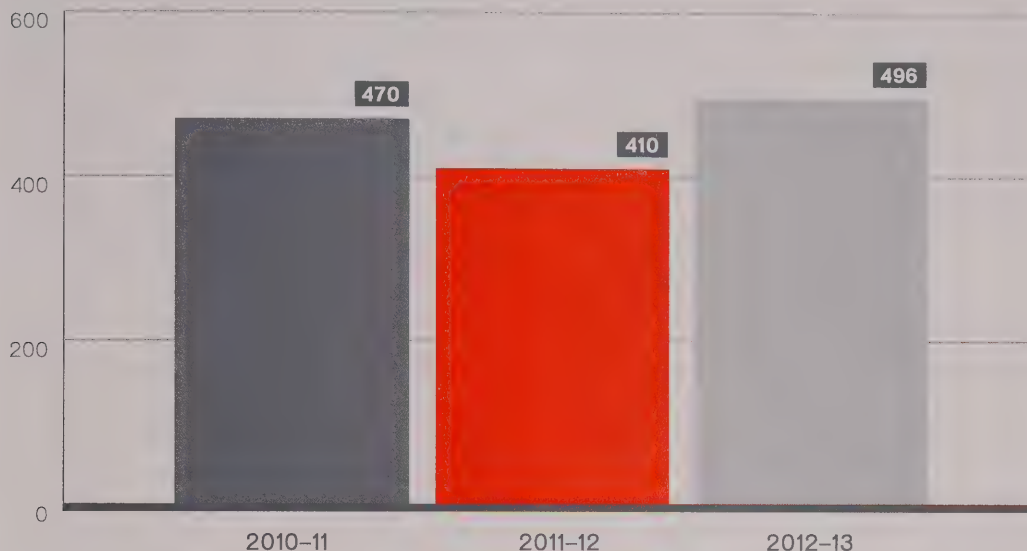
SIRC's Review

This review concentrated on CSIS's new framework and post-2010 investigations. To inform this review, SIRC visited a regional office where there were active investigations related to domestic extremist activities. SIRC was interested in how changes in the Service's approach to domestic extremism affected both national strategy and local investigations. SIRC found the recently revised investigative framework under which the Service is now operating provides more flexibility to collect and report on these threats, regardless of ideology or group membership, and to be logical and sound from the perspective of investigative efficiency. SIRC also examined select files and operational reporting to ensure that investigations were handled in an appropriate and reasonable manner—i.e. that they adhered to internal policy and the CSIS mandate. SIRC found that activities related only to legitimate protest and dissent were not investigated, and that detailed operational reporting on a range of former targets ceased. SIRC also found that CSIS moved quickly to terminate investigation of those individuals who were no longer considered threats after the major events of 2010, and encouraged the Service to be as vigilant regarding future events or issues.

One remaining challenge concerns the inevitable need on the part of the government for information on threats that are mainly inactive today, but which may suddenly rush back to the surface tomorrow;

Targeting

When the Service has reasonable grounds to suspect that an individual or organization could pose a threat to Canada, it must first establish an investigation. This figure indicates the number of targets (rounded to the nearest 10) investigated by CSIS in the past three fiscal years.



the Service must therefore remain abreast of possible flashpoints or triggers that may involve a threat to national security from domestic extremism. In addition, CSIS must ensure that by maintaining this awareness they do not intrude on legitimate forms of protest. Ultimately, it is the Service's partnerships with law enforcement agencies that can act as a potent source of information: law enforcement officials may be aware of individuals involved in ongoing criminal activity who may, at some point, pose a threat according to CSIS's mandate to investigate domestic extremism. SIRC saw examples of fruitful liaison with law enforcement, both in older threats areas where the Service no longer had investigations, and within emerging areas that CSIS needs to be aware of in case a national security nexus develops. Overall, **SIRC encourages the direction the Service is taking in liaising with its domestic partners.**

SIRC REVIEW

CSIS'S USE OF A CLANDESTINE METHODOLOGY

Clandestine methodologies (also frequently referred to as "intelligence tradecraft") include a wide range of specific risk-managed techniques that provide the necessary secrecy and security to assist CSIS in the performance of its duties and functions. As the Service's operations have expanded at home and abroad against increasingly sophisticated targets, there has been a corresponding need to enhance clandestine methodologies to help further protect the identities of its employees, processes and sources of information. This review was concerned with one of these specialized CSIS methodologies.

SIRC's Review

SIRC reviewed relevant documents and spoke to the CSIS employees responsible for the creation, management and ongoing logistics involved with this classified tradecraft. The following key issues were addressed: the justifications for its use; the types of scenarios in which it is applied; the extent of, and SIRC's satisfaction with, the auditing, access and reporting controls used to ensure that the tradecraft is not abused by employees; and finally, an examination of the various relationships that CSIS must maintain to ensure the efficient and effective management of this methodology.

CSIS's Internal Audit Branch had previously performed an assessment on this clandestine methodology and, as such, an additional goal behind SIRC's review was to examine the level to which CSIS responded to the recommendations stemming from that audit. Overall, our review found that CSIS has made many improvements since the audit, including the development of a more comprehensive policy framework and a set of guidelines to better support the expanding use of this covert methodology.

Accountability over the use of this tradecraft is a shared responsibility across CSIS's regional offices. This approach provides regional managers with the necessary flexibility to apply this methodology according to their operational needs, albeit with a sufficient number of headquarters controls, including the creation of a centrally administered database, as well as the formation of a specific unit acting as the policy centre guiding the use of this tradecraft. Prior to CSIS's internal audit, there were a number of challenges associated with financial accountability. SIRC found that additional financial reporting requirements have been put into place and other improvements are underway.

SIRC was informed that there were no instances during the review period in which a CSIS employee was found to have been in violation of security procedures and/or involved in a breach of security with respect to the use of this tradecraft. However, SIRC found there had been one compromise of this covert methodology in recent years, albeit one that

was procedural/administrative in nature and which resulted in no injury or significant risks. The situation was addressed by the appropriate internal stakeholders and the details about the specific compromise were retained on file, as per CSIS policy. As a result, and although generally satisfied with how this compromise was addressed, SIRC found that there was no established procedure requiring that other CSIS regions be informed in a timely manner about the lessons learned following a security breach involving this tradecraft.

In light of this, **SIRC recommends that CSIS policy be changed to ensure that all stakeholders be informed about lessons learned stemming from a suspected or confirmed security breach pertaining to the use of this covert methodology.**

Growing concerns about the need to further safeguard CSIS's employees, processes and sources of information have spurred increased use of this tradecraft. Yet, this in turn has created various management challenges, one of the more pressing being the need to maintain the necessary human resources to ensure its effective use. One solution being developed by CSIS is to utilize a complementary tradecraft/program to help offset this managerial burden. Although this new initiative suggests some promising attributes, SIRC found the policy guiding this accompanying program was insufficient and contradicted tenets of other connected policies. For this reason, **SIRC recommends that CSIS immediately update its policy on the use of this new program so that it is more in line with other operational policies.**

CSIS's use of covert methodologies has come a long way since the creation of the Service in 1984. Indeed, a cornerstone of any successful intelligence agency is to be operationally active without being observed. Without the use of clandestine methodologies, CSIS would not be able to operate effectively nor efficiently. As CSIS embarks on innovative measures to provide greater security to its various activities domestically and abroad, newer challenges will undoubtedly emerge. For this reason, SIRC will be examining other aspects of CSIS's covert methodologies in future reviews.

SIRC REVIEW

THE ROLE OF CSIS IN THE MATTER OF ABOUSFIAN ABDELRAZIK

Background

Abousfian Abdelrazik, a dual Canadian-Sudanese citizen, was arrested by Sudanese authorities in September 2003; he remained in exile in Sudan for six years, unable to secure travel back to Canada. In early 2009, Canadian media reported that his arrest and detention had come at the request of Canadian security intelligence officials, an accusation that CSIS has consistently denied. The allegation also prompted the CSIS Director to publicly write to the Chair of SIRC, asking SIRC to investigate and report on the performance of CSIS's duties and functions with respect to this case.

In the spring of 2011, SIRC launched a review intended to examine CSIS's involvement in the matter of Abousfian Abdelrazik from the months leading up to his departure from Canada for Sudan in March 2003, to his eventual return to Canada. Our review looked at CSIS's investigation of, and interactions with, Abdelrazik both in Canada and abroad, including any role CSIS may have played in his arrest and detention by Sudanese authorities. It also examined the information that CSIS received from, or provided to, domestic and foreign partners in relation to him. More broadly, SIRC explored CSIS's role and advice in the "whole-of-government" approach that was ultimately used in Abdelrazik's case.

Methodology

SIRC requested all relevant information held by CSIS relating to Abdelrazik that fell within the review period, specifically: operational reporting, internal correspondence, and information relating to CSIS's exchanges with domestic and foreign partners. Further to our review of documentation, SIRC submitted questions seeking clarification on a number of issues and asked to speak to certain key individuals who were directly involved in the investigation and management of this case.

As the review unfolded, CSIS apprised SIRC of legal concerns it had arising from the fact that SIRC's review was running concurrent with Abdelrazik's

ongoing civil litigation against the Canadian government. As a result, SIRC's access to the relevant personnel was significantly delayed. Furthermore, CSIS originally provided answers to only some of SIRC's written questions, and, in a number of these cases, those answers were not complete. After extensive internal deliberation and consultation, it was reiterated to CSIS that SIRC's mandated activities and any ongoing court proceedings were distinct and separate processes, with neither affecting nor impeding the progress of the other.

In time, SIRC did receive full answers and full cooperation from the Service. SIRC was also ultimately able to speak with several of the key persons involved in the file, although the passage of time since the original events meant that some of these individuals no longer worked for the Service. In light of the delays we encountered, SIRC chose to narrow the primary focus of its review: it mostly scrutinizes the earlier phase of this case (specifically, from March 2003 to December 2004), which corresponded to CSIS's most intense involvement. Following that period, Abdelrazik's case became much more complex, and began to draw a number of other Canadian agencies into significant roles.

Because of the nature of the issue and the direct and public request by the former CSIS Director, the Committee decided to submit its report directly to the Minister of Public Safety under Section 54 of the *CSIS Act*.

Findings

SIRC found no indication that CSIS had requested Sudanese authorities to arrest or detain Abousfian Abdelrazik. CSIS did, however, in the months leading up to Abdelrazik's departure and eventual arrest abroad, keep its foreign intelligence allies up to date on any fresh information gleaned from their investigation of him.

As this case unfolded, SIRC found that Sudanese authorities remained under the mistaken impression that Canada, including CSIS, had supported the original decision to arrest and detain Abdelrazik. This confusion could perhaps be explained by the fact that the genesis of this case put it front and centre as an intelligence issue, and it remained so (according

to reporting) in the minds of the Sudanese. Further complicating matters was the fact that, originally, the two Canadian government agencies most heavily involved in this case—DFAIT and CSIS—carried out their respective consular and intelligence work concurrently, though sometimes at odds with each other. SIRC's review concluded that upon learning of Abdelrazik's detention in Sudan, CSIS should have been more forthcoming with DFAIT in regards to what it knew so as to ensure a more informed and coordinated Canadian response to this case.

SIRC's review did raise a number of concerns. First, following Mr. Abdelrazik's initial incarceration, CSIS was allowed to interview him in Sudan. CSIS followed proper authorities in seeking approval for conducting this interview; SIRC found, however, that in the context of its interview and its subsequent report, CSIS inappropriately and, in contravention of CSIS policy, disclosed personal and classified information.

Second, in mid-2004, and in preparation for Mr. Abdelrazik's possible release, CSIS updated its government partners on information the Service possessed. Although these updates would not be the final word concerning the Service's assessment of the situation, and although it would be years before Abdelrazik left Sudan (thus mitigating the impact of what the assessments had asserted), SIRC found that these assessments contained exaggerated and inaccurately conveyed information.

Third, SIRC had concerns with respect to CSIS's investigation, notably, that CSIS excessively reported, and hence retained in its operational databases, a significant amount of information not related to the threat, originating from individuals who were not targets.

Preparing Our Report

SIRC has found it challenging to put the findings of this review into the appropriate context. It has been nearly a decade since Abdelrazik first left Canada for the Sudan, and it is an understatement to note that since the events of 2003 and 2004, much has changed in Canada's security and intelligence landscape.

To begin, multiple Canadian Commissions of Inquiry, including the O'Connor (2006), Iacobucci (2008) and Major (2010) reports have commented extensively on a wide spectrum of security and intelligence issues. Although not related directly to Abdelrazik's case, the numerous recommendations flowing from these inquiries attempted to improve the professional standards expected of the government departments and agencies generally involved in security and intelligence matters and, in many cases, were directed specifically at improving the policies and practices of CSIS.

Another consideration is the wide spectrum of jurisprudence that has steadily been developed over the past decade and which comments on the roles and responsibilities of government(s), citizens and immigrants (permanent residents) when national security is the fulcrum of debate. Pointedly, Mr. Abdelrazik's own stilted progression through Canada's legal system is well publicized, such that it does not require repeating here.

For its part, SIRC has not been an idle bystander as the preceding tumultuous decade unfolded. In fact, many of the Committee's previous recommendations have covered issues that are germane to the Abdelrazik case. Some of these include:

- ▼ That CSIS, in its collection of information, avoid extensive reporting of non-targeted individuals (cf. SIRC 2002–2003 annual report: Domestic Threats in Conjunction with Lawful Advocacy, Protest and Dissent);
- ▼ That CSIS amend operational policy outlining the procedures for documenting contact with agencies known or reputed to have engaged in human rights abuses (cf. SIRC 2005–2006 annual report: CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post);
- ▼ That CSIS review its use of investigative techniques to ensure they reflect established best practices (cf. SIRC 2005–2006 annual report: Electronic Surveillance and Information-Gathering Techniques);

- ▼ That CSIS and DFAIT update their MOU to designate the latter as the lead agency in cases involving Canadian citizens detained abroad, including reflecting the protocol, described by Justice O'Connor, of "timely and open consultation among Canadian agencies" involved with Canadians detained abroad; and "a coherent and unified approach," led by DFAIT; and "accountability for the course of action adopted" in such cases (cf. SIRC 2006–2007 annual report: *The Case of Mohammed Mansour Jabarah*);
- ▼ That CSIS implement measures to embed the values stemming from recent political, judicial and legal developments in its day-to-day work in order to maintain its own credibility, and to meet growing and evolving expectations of how an intelligence agency should operate and perform in a contemporary democratic society, and that CSIS seek guidance and advice from the Minister (cf. SIRC 2008–2009 annual report: *The Role of CSIS in the Case of Omar Khadr*);
- ▼ That CSIS adopt a broader interpretation of its disclosure commitments to DFAIT (cf. SIRC annual report 2010–2011: *CSIS Relationships with Partners*).

When considered holistically, these points and other SIRC recommendations have fundamentally affected how CSIS conducts its business, including the implementation of new ministerial direction and policies guiding CSIS's information collection, retention, analysis and dissemination functions, as well as how the Service's relationships with domestic and foreign agencies are expected to be managed. As a result, CSIS's entire program of operations—both at home and, especially, abroad—do not resemble what it was in the years focused upon in this review.

Perhaps of equal importance is the fact that Abdelrazik's case became much broader and more complex as the years went by: at the same time as CSIS's investigation of him was significantly reduced (given his apparent indefinite inability to leave Sudan), a raft of other Canadian government departments—notably

DFAIT, the RCMP, CBSA and Transport Canada—(as well as foreign government agencies) commenced wrestling over his fate. SIRC is unable to ascertain the extent to which any of these entities may or may not have acted on CSIS's advice, or to what extent CSIS information factored into the decision-making of others. Indeed, SIRC has no review jurisdiction beyond CSIS and, therefore, had to limit its commentary to what the Committee knows solely as it pertained to the Service's involvement.

Conclusions

For all of these reasons, SIRC elected not to present any recommendations to policy or practice as part of this review. Indeed, most of the relevant CSIS policies have already changed, and/or operational practices have evolved over the past decade, meaning that SIRC would, in effect, be resubmitting recommendations already covered by Commissions of Inquiry or by decisions of Canadian courts or the Committee itself.

Nonetheless, we believe there are a number of valuable lessons to be drawn from SIRC's review of CSIS's role in the case of Abousfian Abdelrazik. That CSIS produced threat assessments based on incorrect and exaggerated information should be of concern, as should the fact that classified information was improperly provided, despite existing policy and specific preventative senior management direction. There are also important concerns in regard to CSIS's relationship with its Government of Canada partners, especially, in this case, DFAIT.

As SIRC has pointed out in a range of recent studies (with some of the pertinent recommendations cited above), CSIS is rapidly expanding abroad and is becoming a much more frequent and integrated partner with other large government agencies. As it pursues that role, however, CSIS will be facing the increased responsibilities and expectations that accompany them. For example, CSIS told SIRC in 2012 that existing legislation and MOUs "allow but do not require" CSIS to share information that would be of critical importance

to the work of government partners; that statement is technically correct but greatly minimizes—if not undermines—the entire intention of fostering closer and more integrated working relationships among government agencies. SIRC strongly encourages CSIS to view this report as a detailed retrospective, and an opportunity to re-evaluate its posture and approach to being party to a whole-of-government approach.

On a final note, the inability of this study to move beyond the confines of CSIS is a limitation on which this Committee has publically commented previously. Although the 1984 Special Senate Committee, which reviewed the draft legislation that would become the *CSIS Act*, anticipated SIRC would provide a “vital role in the functioning of the security intelligence system” by promoting “adequate debate, where necessary, in the area of security,” this function is curtailed by the practical limitations of our mandate.

Therefore, although we stand by our review of CSIS’s role in the Abdelrazik case, this study does not constitute the definitive or complete picture on this subject. Other information is likely to emerge from the broad range of documents or reports held by other Government of Canada departments and agencies that were equally involved, as well as from ongoing legal processes. As it stands, Abousfian Abdelrazik’s story has yet to be fully written.

CERTIFICATION OF THE DIRECTOR OF CSIS’S ANNUAL REPORT TO THE MINISTER OF PUBLIC SAFETY: OVERVIEW

As per its new statutory requirements, SIRC engaged in the certification of the Director of CSIS’s annual report to the Minister of Public Safety. The statements required by Section 38(2) of the *CSIS Act* amount to significant assurances regarding the legality, reasonableness and necessity of the Service’s operational activities. Moreover, the Director’s report has been, in recent years, a useful and comprehensive overview of the whole of CSIS operations. The report for fiscal year 2011–2012 was no exception, and it provided a summary of the major operational accomplishments and challenges faced by the Service over the previous year. As a result, SIRC found that certifying the “operational activities described in the report” meant certifying a high-level description of almost the whole of CSIS’s activities for fiscal year 2011–2012.

With the exception of three issues, SIRC is satisfied with the Director’s report on the Service’s operational activities for the 2011–2012 reporting period. In addition, it is SIRC’s opinion that the operational activities, as they are described in the Director’s report, did not contravene the *CSIS Act* or ministerial directives, nor did they involve the unreasonable or unnecessary use of the Service’s powers.

CHANGES TO THE *CSIS ACT*

In 2012, the Government of Canada amended the *CSIS Act* to require that SIRC complete some of the responsibilities formerly assigned to the Inspector General of CSIS. Primary among these was the requirement that SIRC submit to the Minister of Public Safety a certificate stating the degree to which the Committee is satisfied with the report. In addition, SIRC is to discuss whether any of the Service’s operational activities described in the report were not authorized by the *CSIS Act*, contravened any ministerial directions issued under the *Act*, or involved any unreasonable or unnecessary exercise of the Service’s powers.

Satisfaction with the Report

The purpose of the Director's report, submitted pursuant to Section 6(4) of the *CSIS Act*, is to provide the Minister with information to assist him in exercising ministerial responsibility for CSIS. Accordingly, SIRC's satisfaction with the report was based on whether the Director's report fulfilled that function. SIRC measured this against three criteria: first, whether the report met the ministerial reporting requirements set out in the 2008 Ministerial Directives on Operations and the 2011–2012 Ministerial Directives on Intelligence Priorities; second, whether the report was factually accurate; and, third, whether, in SIRC's opinion, the report provided an accurate representation of CSIS activities during the 2011–2012 fiscal year.

With respect to ministerial reporting requirements, SIRC found that the Director's report addressed them all but one. During the certification process, SIRC learned that although this issue was not specifically addressed in the Director's report, the Service did provide the Minister with this information as part of a Memorandum to Cabinet. Accordingly, this omission did not detract from SIRC's overall satisfaction with the Director's report.

Regarding the accuracy of the Director's report, SIRC is of the opinion that the information provided by the Director's report was, on the whole, factually accurate. SIRC reviewed the statements in the report against CSIS information holdings, and, where warranted, SIRC submitted written requests for additional documentation and clarification. On the basis of this review, SIRC determined that, with the exception of two statements, the Director's report was fully supported and appropriately documented. The errors identified related to the inaccurate characterization of the status of the Service's relationship with another agency and the omission of one operation from the total number of these types of operations.

SIRC considered whether the Director's report provided an accurate representation of CSIS activities during the 2011–2012 reporting period. To make this determination, SIRC submitted written requests for information on CSIS operational activities. This included requests for statistics on the Service's core activities such as targeting, human source operations and warrant applications as well as information on foreign and domestic liaisons, technical and operational support, foreign operations and security screening. The Service's responses enabled SIRC to construct a comprehensive picture of the extent of Service activities, and permitted SIRC to assess the Director's report against this bigger picture.

SIRC found that the Director's report was a useful and comprehensive overview of the whole of CSIS operations. Nevertheless, SIRC determined that the Director's report did not contain a detailed description of the Service's activities in support of Section 16 collection of information concerning foreign states and persons. As these activities are an integral part of the Service's operations, SIRC believes that a more detailed description was warranted.

SIRC also found that the Director's report did not contain a sufficiently detailed description of the Service's foreign operations. SIRC is of the opinion that more detailed information would have provided a more accurate and representative description of the Service's foreign operations and would help provide the Minister with a better understanding of the elevated threats to the lives of Service employees in this environment. As such, the Director may wish to consider including such information in next year's report; SIRC believes that this issue is of sufficient concern that it warrants the Minister's attention and continued consideration.

Compliance with the *CSIS Act* and Ministerial Directives, and Exercise of Service Powers

In addition to requiring SIRC to state its satisfaction with the Director's report, Section 38(2) of the *CSIS Act* requires SIRC to state whether, in its opinion, the operational activities described in the Director's report contravened the *Act* or ministerial directives and whether the activities involved any unreasonable or unnecessary use of the Service's powers.

To make this assessment, SIRC conducted an extensive examination of the review environment. This included a review of recent changes to the *CSIS Act*, the authorities for the Service to collect Section 16 information, and relevant ministerial directives and intelligence priorities. It also included an examination of the Service's internal governance framework, including internal directives and the Service's operational policies.

SIRC found that, with one exception, the Service's internal governance structure upholds the *CSIS Act* and ministerial directives. SIRC determined that the Service's practice of sharing information with domestic and foreign signals intelligence (SIGINT) agencies is potentially problematic in terms of compliance with ministerial directives on information

sharing. This was not an issue that came to light during the certification process exclusively. Rather, it first came to light in the context of a SIRC review entitled "CSIS's Relationship and Exchanges with Communications Security Establishment Canada," which examined the issue during the period covered by the 2011–2012 Director's report. For the purposes of certifying the Director's report, SIRC did not characterize this issue as an instance of non-compliance with ministerial directives. Nevertheless, SIRC believes that it is of sufficient concern that it warrants the Minister's consideration.

With the exception of this one area, SIRC is of the opinion that the activities, as they are described in the report, comply with the *Act* and ministerial directives and constituted a reasonable and necessary exercise of the Service's powers. Specifically, SIRC determined that the activities described in the report were consistent with the duties and functions specified in sections 12 to 20 of the *CSIS Act* and complied with relevant Section 16 requests from the Ministers of Department of Foreign Affairs and National Defence, and with ministerial directives on operations, information sharing and intelligence priorities.

B. COMPLAINTS

In addition to its review function, SIRC conducts investigations into complaints concerning CSIS made by either individuals or groups. The types of complaints that SIRC investigates are described in the *CSIS Act* and can take several forms, although two predominate. Under Section 41 of the *CSIS Act*, SIRC investigates “any act or thing done by the Service.” Under Section 42, SIRC investigates complaints about denials or revocations of security clearances to federal government employees and contractors. Far less frequently, SIRC conducts investigations in relation to referrals from the Canadian Human Rights Commission, or Minister’s reports in regards to the *Citizenship Act*.

The Complaints Process at SIRC

Complaint cases may begin as inquiries to SIRC either in writing, in person or by phone. Once a written complaint is received, SIRC staff will advise a prospective complainant about what the *CSIS Act* requires to initiate a formal complaint.

Once a formal complaint is received in writing, SIRC conducts a preliminary review. This can include any information that might be in the possession of CSIS, except for Cabinet confidences. Where a complaint does not meet certain statutory requirements, SIRC declines jurisdiction and the complaint is not investigated.

If jurisdiction is established, complaints are investigated through a quasi-judicial hearing presided over by one or more Committee Members. They are assisted by staff and by SIRC’s legal team, which provides legal advice to Members on procedural and substantive matters.

Pre-hearing conferences may be conducted with the parties to establish and agree on preliminary procedural matters, such as the allegations to be investigated, the format of the hearing, the identity and number of witnesses to be called, the production of documents in advance of the hearing and the date and location of the hearing.

The time to investigate and resolve a complaint will vary in length depending on a number of factors, such as the complexity of the file, the quantity of documents to be examined, the number of hearing days required (both in the presence and the absence of the complainants), and the availability of the participants.

The *CSIS Act* provides that SIRC hearings are to be conducted “in private.” All parties have the right to be represented by counsel and to make representations at the hearing, but no one is entitled as of right to be present during, to have access to, or to comment on, representations made to SIRC by any other person.

A party may request an *ex parte* hearing (in the absence of the complainant and possibly other parties) to present evidence which, for reasons of national security or other reasons considered valid by SIRC, cannot be disclosed to the other party or their counsel. During such hearings, SIRC’s legal team will cross-examine the witnesses to ensure that the evidence is appropriately tested and reliable. This provides the presiding Member with the most complete and accurate factual information relating to the complaint.

Once the *ex parte* portion of the hearing is completed, SIRC will determine whether the substance of the evidence can be disclosed to the excluded parties. If so, SIRC will prepare a summary of the evidence and provide it to the excluded parties once it has been vetted for national security concerns.

When SIRC’s investigation of a complaint made under Section 41 is concluded, it provides a report to the Director of CSIS and to the Minister of Public Safety, as well as a declassified version of the report to the complainant. In the case of a complaint under Section 42, SIRC will also provide its report to the Deputy Head concerned.

Table 1 provides the status of all complaints directed to SIRC over the past three fiscal years, including complaints that were misdirected to SIRC, deemed to be outside SIRC's jurisdiction, or investigated and resolved without a hearing (i.e. via an administrative review).

TABLE 1: COMPLAINTS DIRECTED TO SIRC

	2010-11	2011-12	2012-13
Carried over	31	16	22
New	17	17	17
TOTAL	48	33	39
Closed†	32	11	14

† Closed files include those where reports were issued, where the Committee did not have jurisdiction, where the preliminary conditions of the complaint were not met, or where the complaint was discontinued

HOW SIRC DETERMINES JURISDICTION OF A COMPLAINT...

...under Section 41

Under Section 41 of the *CSIS Act*, SIRC shall investigate complaints made by “any person” with respect to “any act or thing done by the Service.” Before SIRC investigates, two conditions must be met:

- 1** The complainant must first have complained in writing to the Director of CSIS and not have received a response within a reasonable period of time (approximately 30 days), or the complainant must be dissatisfied with the response; and
- 2** SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

SIRC cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Labour Relations Act*.

...under Section 42

With respect to security clearances, Section 42 of the *CSIS Act* says SIRC shall investigate complaints from:

- 1** Any person refused federal employment because of the denial of a security clearance;
- 2** Any federal employee who is dismissed, demoted, transferred or denied a transfer or promotion for the same reason; and
- 3** Anyone refused a contract to supply goods or services to the government for the same reason.

These types of complaints must be filed within 30 days of the denial of the security clearance.

SIRC may extend this period if valid reasons are presented.

SIRC INVESTIGATION

ALLEGED HARASSMENT, RACIAL PROFILING AND SHARING OF MISLEADING INFORMATION

SIRC investigated a complaint under Section 41 of the *CSIS Act* in which the complainant alleged that a CSIS employee had, during an interview with him, conducted himself in a manner that constituted harassment, used inappropriate interview tactics, made threats and lied about the impact of the interview on the complainant's security clearance. He also alleged that CSIS was using racial profiling and that other CSIS employees, during interviews in relation to the government security clearance assessment process, had interfered with his freedom of religion. Finally, the complainant further alleged that CSIS's investigation for his security clearance assessment was inadequate, had led to the sharing of misleading information about him with a government department, and had been marred by undue delay.

SIRC found that the first CSIS employee's conduct amounted to neither harassment nor inappropriate tactics, but that his choice of discussion topics and tone had created unnecessary tension at the interview. SIRC also found that the employee was deceptive in that he did use the security clearance process as a ruse to get the complainant to provide information. **SIRC made recommendations to CSIS to address this issue at an operational and policy level to minimize the likelihood of such a scenario occurring again.**

SIRC found that there was no evidence of racial profiling in this case and that CSIS was fully justified in pursuing its security screening investigation of the complainant as it did on the basis of the information it had in order to fulfill its mandate. Nevertheless, SIRC also found that it is not unreasonable for people, such as the complainant, who don't have access to classified information, to perceive that they are being profiled. In this respect, **SIRC recommends that CSIS engage in outreach with minority communities to explore the issue of racial data collection as a possible way to reassure the public that CSIS does not racially profile individuals.**

SIRC found that there was no interference with freedom of religion in the context of the government security clearance assessment process, and that CSIS's

investigation was adequate under the security screening policy in force. SIRC found the allegation of undue delay to be unfounded.

While SIRC did not find that CSIS shared misleading information about the complainant, SIRC estimated that the information provided to the other government department was incomplete in that it excluded some of the assessment's findings. **SIRC recommends that CSIS remedy the situation by sending the previously excluded information to the department concerned.**

Finally, the complainant also alleged that there were many examples of profiling in documents about him produced internally by the other department concerned following the sharing of information from CSIS, and that the same department had failed to formally deny his clearance application, thereby preventing him from seeking a remedy under Section 42 of the *CSIS Act*. Because of the limitations on SIRC's mandate in this investigation under Section 41 of the *CSIS Act*, SIRC was not able to make findings on this issue.

SIRC INVESTIGATION

ALLEGED DENIAL OF BASIC RIGHTS AND INSUFFICIENT CULTURAL KNOWLEDGE

SIRC investigated a complaint under Section 41 of the *CSIS Act* in relation to the conduct of a CSIS employee at a permanent resident application-screening interview. The complainant alleged that the CSIS employee had denied him certain basic rights, had behaved improperly, and lacked sufficient knowledge of the complainant's cultural background and country of origin.

SIRC found that, while no rights of the complainant had been violated, the CSIS employee should have shown flexibility to accommodate certain demands of the complainant at the interview. Similarly, SIRC did not find evidence of improper conduct on the part of the employee, but it did find that the employee, in one instance, could have been more sensitive to the complainant's apprehensions. SIRC reminded CSIS that its employees should show sensitivity when interviewing persons who come from countries where intelligence agencies are feared, and should avoid any actions that could be construed as crossing the line or as being manipulative.

SIRC also found that the CSIS employee was adequately prepared before entering the interview, and that his knowledge of the complainant's culture and country was sufficient.

Finally, to avoid rescheduling immigration interviews and causing further undue delay, SIRC recommends that CSIS issue an operational directive to all regional offices, consistent with the direction taken by the Toronto region, requiring investigators to take recording devices to all immigration interviews, and to ensure that such devices are in working order.

SIRC INVESTIGATION

ALLEGED DELAY IN PROVIDING A SECURITY ASSESSMENT

SIRC investigated a complaint under Section 41 of the *CSIS Act* regarding the alleged delay by CSIS in providing its security assessment for the complainant's site access clearance. The complainant argued that the delay had caused him to lose work opportunities.

SIRC found that the process, decisions and actions taken by CSIS in the course of the assessment were reasonable. The case officer and investigator afforded attention to details to ensure that the assessment was appropriate.

Notwithstanding the above, SIRC found that there were delays and periods of inactivity on the file which, when added together, rendered the overall delay unreasonable. SIRC reiterated a past

recommendation that a tracking system be put in place to identify files falling outside average processing times to ensure that priority be given to such files. In addition, **SIRC recommends that time management systems and reminders be implemented to avoid such situations.**

SIRC INVESTIGATION

REVOCATION OF SECURITY CLEARANCES

SIRC separately investigated two related complaints under Section 42 of the *CSIS Act* made by complainants who were government employees and whose security clearances had been revoked on the basis of their association with a third-party entity.

SIRC found that there were reasonable grounds to question the complainants' reliability as it relates to loyalty on the basis of the complainants' associations with persons or groups of concern. In this respect, the complainants could act or be induced to act in a way that would constitute a threat to the security of Canada. **For these reasons, SIRC recommends that the decision to revoke the complainants' security clearances be upheld.**

Also as a result of these investigations, **SIRC recommends the review of certain policy guidelines for employees on the issue of what they can disclose to third parties with respect to the identity of their employer, recommending a more consistent policy that defines the situations where such disclosure is appropriate.**

SECTION 3

SIRC AT A GLANCE

COMMITTEE MEMBERSHIP

SIRC is chaired by the Honourable Chuck Strahl, P.C. The other Committee Members are: the Honourable Frances Lankin, P.C., C.M.; the Honourable Denis Losier, P.C., C.M.; the Honourable Deborah Grey, P.C., O.C.; and the Honourable L. Yves Fortier, P.C., C.C., O.Q., Q.C.

STAFFING AND ORGANIZATION

SIRC is supported by an Executive Director, Michael Doucet, and an authorized staff complement of 17, located in Ottawa. This includes a Director of Research, a Senior Counsel, a Corporate Services Manager and other professional and administrative staff.

The Committee, in consultation with staff, approves direction on research and other activities that are identified as a priority for the year. Management of day-to-day operations is delegated to the Executive Director with direction, when necessary, from the Chair as Chief Executive Officer.

As part of their ongoing work, the Chair of SIRC, Committee Members and senior staff participate in regular discussions with the CSIS executive and staff, and other members of the security intelligence community. These exchanges are supplemented by discussions with academics, security and intelligence experts and other relevant organizations. Such activities enrich SIRC's knowledge about issues and debates affecting Canada's national security landscape.

Committee Members and, especially, SIRC staff, also visit CSIS regional offices to understand and assess the day-to-day work of investigators in the field. These visits give SIRC an opportunity to be briefed by regional CSIS staff on local issues, challenges and priorities. They also provide an opportunity to communicate SIRC's focus and concerns.

With respect to human resources, SIRC continues to manage its activities within allocated resource levels. Staff salaries and travel within Canada for Committee hearings, briefings and review activities represent its chief expenditures.

Table 2 below presents a breakdown of actual and estimated expenditures.

TABLE 2: SIRC EXPENDITURES 2012-13 (\$ THOUSANDS)

	2012-13 (Tot. Auth.)	2012-13 (Actual)
Personnel	2,349	2,050
Goods and services	732	852
Total	3,081	2,901

SIRC ACTIVITIES

May 27-30, 2012: SIRC co-hosted the International Intelligence Review Agencies Conference (IIRAC), along with the Office of the Communications Security Establishment Commissioner. Under the theme “Strengthening Democracy Through Effective Review,” the conference reunited delegates from Australia, Belgium, Germany, the Netherlands, Norway, South Africa, the United Kingdom and the United States. The conference was held at Ottawa’s Château Laurier, and featured panels on Legal Development in Review and Oversight, Media as a Form of Review/Oversight, Engaging the Public, and Balancing National Security and Individual Rights. Featured speakers for the conference included Senator Hugh Segal, Mel Cappe (former Clerk of the Privy Council), Jim Judd (former Director of CSIS), David Walmsley (Managing Editor of the *Globe and Mail*), and Federal Court Justice Simon Noël, among many others.

July 23-27, 2012: The Executive Director, along with representatives from CSIS, the Department of Justice, and Foreign Affairs and International Trade Canada, participated in a capacity-building exercise in Trinidad and Tobago.

October 11, 2012: SIRC’s Executive Director met with a delegation of the French government in Ottawa, including the coordonnateur national du renseignement.

November 19-20, 2012: SIRC Chair and Committee Members visited CSIS’s British Columbia and Prairie regional offices.

January 22, 2013: The Executive Director met, in a follow-up meeting, with members of the Délégation parlementaire française – Contrôle de la communauté du renseignement, in Ottawa.

February 6-8, 2013: The Executive Director attended the 14th Annual Privacy and Security Conference in Victoria, British Columbia.

March 27-28, 2013: The Executive Director attended the Institute on Governance’s Public Governance Exchange Conference.

LIST OF SIRC RECOMMENDATIONS

During the 2012–2013 review period, SIRC made the following recommendations stemming from the reviews it conducted, as well as from the complaints it investigated.

REPORT	SIRC RECOMMENDATIONS
CSIS's Relationship and Exchanges with CSEC	SIRC recommends that CSIS develop clearer and more robust overarching principles of cooperation with CSEC. These principles should address the growing volume of challenges that have arisen between the two agencies, while respecting the individual mandates of each organization.
Review of a New Section 21 Warrant Power	SIRC recommends that CSIS extend the use of caveats and assurances in regards to this new warrant power to include the agencies of the entire Five Eyes community.
Investigating Activities Related to Espionage and Foreign Influence	SIRC recommends that CSIS carry out the appropriate fine-tuning, in policy and practice, to assist investigators and analysts in identifying common and consistent thresholds, and in judging when an activity has crossed over into the clandestine realm. SIRC also recommends that CSIS develop a strategy to deliver the same cautionary messages about foreign-influenced activities for all potentially affected sectors.
CSIS Initiatives for Foreign Collection	SIRC recommends continued support for the development of operational training, and that the Service ensure that all persons who are identified as a priority for training receive it, particularly if they are operating in a dangerous environment. SIRC also recommends that CSIS develop a legal framework outlining acceptable and prohibited activities, including the corresponding levels of approval within and outside the Service.
CSIS's Evolving Footprint Abroad	SIRC recommends that CSIS take immediate action to ensure that Section 17 profiles are consistently accurate, complete, up-to-date and relevant.
CSIS's Support to Canada's Northern Perimeter	SIRC recommends that CSIS "institutionalize responsibility" for northern initiatives by setting out headquarters-driven liaison and operational objectives over a multi-year period, and ensure that these objectives are sustained with an appropriate resource commitment.
CSIS's Use of a Clandestine Methodology	SIRC recommends that CSIS policy be changed to ensure that all stakeholders be informed about lessons learned stemming from a suspected or confirmed security breach pertaining to the use of this covert methodology. SIRC also recommends that CSIS immediately update its policy on the use of this new program so that it is more in line with other operational policies.
Alleged Harassment, Racial Profiling and Sharing of Misleading Information by CSIS	SIRC recommends that CSIS engage in outreach with minority communities to explore the issue of racial data collection as a possible way to reassure the public that CSIS does not racially profile individuals. SIRC also recommends that CSIS remedy the situation by sending the previously excluded information to the department concerned.

REPORT	SIRC RECOMMENDATIONS
<p>Alleged Denial of Basic Rights and Insufficient Cultural Knowledge on the Part of CSIS</p>	<p>To avoid rescheduling immigration interviews and causing further undue delay, SIRC recommends that CSIS issue an operational directive to all regional offices, consistent with the direction taken by the Toronto region, requiring investigators to take recording devices to all immigration interviews, and to ensure that such devices are in working order.</p>
<p>Alleged Delay in Providing a Security Assessment</p>	<p>SIRC recommends that time management systems and reminders be implemented to avoid such situations.</p>
<p>Revocation of Security Clearances</p>	<p>SIRC recommends that the decision to revoke the complainants' security clearances be upheld.</p> <p>SIRC also recommends the review of certain policy guidelines for employees on the issue of what they can disclose to third parties with respect to the identity of their employer, recommending a more consistent policy that defines the situations where such disclosure is appropriate.</p>

RAPPORT		RECOMMANDATIONS DU CSARS	
<p>Allegations de harcèlement, de profilage racial et de partage de données trompeuses</p>	<p>Le CSARS recommande au SCRS de communiquer avec les communautés minoritaires pour aborder la question de la collecte des données concernant l'origine ethnique, et ce, comme un moyen possible de rassurer le public sur le fait que le SCRS ne fait pas de profilage racial.</p> <p>Le CSARS recommande que le SCRS remédie à la situation en envoyant les informations précédemment exclues au ministère concerné.</p>	<p>Allegations de refus des droits fondamentaux et de connaissances culturelles insuffisantes de la part du SCRS</p>	<p>Le CSARS recommande qu'enfin d'éviter de reporter les entrevues d'immigration et de causer des retards supplémentaires excessifs, le SCRS émette une directive opérationnelle à tous les bureaux régionaux, conformément avec l'orientation prise par la région de Toronto, selon laquelle les enquêteurs sont tenus d'amener des appareils d'enregistrement à toutes les entrevues d'immigration et de veiller à ce qu'ils soient en état de marche.</p>
<p>Allegations de retard à fournir une évaluation de sécurité</p>	<p>Le CSARS recommande que des systèmes de gestion du temps et des rappels soient mis en œuvre pour éviter de telles situations.</p>	<p>Allegations de révoquant d'habilités de sécurité</p>	<p>Le CSARS recommande que la décision de révoquer les habilitations de sécurité des plaignants soit maintenue.</p> <p>Le CSARS recommande la révision de certaines lignes directrices de politiques pour les employés sur la question de ce qu'ils peuvent divulguer à des tiers en ce qui concerne l'identité de leur employeur, et a conseillé une politique plus cohérente définissant les situations où une telle divulgation est appropriée.</p>

LISTE DES RECOMMANDATIONS DU CSARS

Àu cours de la période étudiée, l'exercice 2012-2013, le CSARS a formulé les recommandations qui suivent découlant des études effectuées et des plaintes visées par ses enquêtes.

RECOMMANDATIONS DU CSARS	RAPPORT
<p>Le CSARS recommande que le SCRS élabore des principes généraux de coopération avec le CSTC plus clairs et plus solides. Ces principes devraient répondre au nombre croissant de défis qui ont surgi entre les deux organisations, tout en respectant leurs mandats respectifs.</p> <p>Le CSARS recommande que, dans le cadre de ce nouveau pouvoir octroyé au moyen de mandat, le SCRS étende l'usage de mises en garde et de garanties aux organismes de toute la communauté du Groupe des cinq.</p>	<p>Les relations et échanges du SCRS avec le CSTC</p> <p>Examen du nouveau pouvoir octroyé au moyen de mandat en vertu de l'article 21</p>
<p>Le CSARS recommande que le SCRS réajuste de façon appropriée ses politiques et pratiques, et ce, pour aider les enquêteurs et analystes à identifier des seuils communs et cohérents, et pour évaluer quand une activité passe dans le domaine clandestin.</p> <p>Le CSARS recommande que le SCRS élabore une stratégie visant à offrir les mêmes messages d'avertissement sur les activités influencées par l'étranger à tous les secteurs potentiellement touchés par de telles activités.</p> <p>Le CSARS soutient le développement de la formation opérationnelle, et recommande que le Service veille à ce que toutes les personnes jugées prioritaires pour la formation en bénéficient, surtout si elles travaillent dans un milieu dangereux.</p> <p>Le CSARS recommande que le SCRS élabore un cadre juridique décrivant les activités acceptables et interdites, notamment les niveaux d'approbation correspondants au sein même du Service et en dehors de celui-ci.</p>	<p>Le travail d'enquête liée à l'espionnage et à l'influence étrangère</p> <p>Les initiatives du SCRS en matière de collecte à l'étranger</p>
<p>Le CSARS recommande que le SCRS prenne des mesures immédiates pour s'assurer que les profils en vertu de l'article 17 sont toujours exacts, complets, à jour et pertinents.</p>	<p>L'évolution de la marque du SCRS à l'étranger</p>
<p>Le CSARS recommande que le SCRS « institutionnalise les responsabilités » en matière d'initiatives dans le Nord, et ce, en demandant au siège du Service d'établir des objectifs de liaison et opérationnels sur plusieurs années. Le Service doit aussi s'assurer que des ressources sont engagées à l'appui de tels objectifs.</p>	<p>L'appui du SCRS au périmètre de sécurité du Nord du Canada</p>
<p>Le CSARS recommande que la politique du SCRS soit modifiée pour s'assurer que toutes les parties sont informées des leçons apprises à la suite d'une infraction de la sécurité suspectée ou confirmée concernant l'usage de cette méthode secrète.</p> <p>Le Comité recommande également que le SCRS mette immédiatement à jour sa politique sur ce nouveau programme afin qu'elle soit plus en phase avec les autres politiques opérationnelles.</p>	<p>Le recours du SCRS aux méthodes clandestines</p>

Le tableau 2 présente une ventilation des dépenses réelles et des prévisions de dépenses.

TABLEAU 2 : DÉPENSES DU CSARS 2012-2013 (EN MILLIERS DE DOLLARS)

2012-2013 (total des autorisations)	2012-2013 (réelles)		
		Personnel	Biens et services
2 349	2 050		
732	852		
3 081	2 901		
		Total	

ACTIVITÉS DU COMITÉ

27-30 mai 2012 : Le CSARS a tenu la conférence internationale des organismes de surveillance du renseignement, de concert avec le Bureau du Commissaire du Centre de la sécurité des télécommunications. Cette conférence, qui avait pour thème « consolider la démocratie par une surveillance efficace », a réuni à l'hôtel Château Laurier d'Ottawa des délégués de l'Australie, de la Belgique, de l'Allemagne, des Pays-Bas, de la Norvège, de l'Afrique du Sud, du Royaume-Uni et des États-Unis. Elle présentait des groupes d'experts sur l'évolution du droit dans divers domaines : la surveillance et le contrôle, les médias comme moyen de surveillance/contrôle, la mobilisation de l'opinion publique et l'équilibre entre la sécurité nationale et les droits individuels. Parmi les conférenciers invités, on comptait le sénateur Hugh Segal, Mel Cappe (ancien greffier du Conseil privé), Jim Judd (ancien directeur du SCRS), David Walmsley (rédacteur en chef du *Globe and Mail*) et le juge Simon Noël, de la Cour fédérale.

23-27 juillet 2012 : La directrice exécutive, accompagnée de représentants du SCRS, du ministère de la Justice ainsi que d'affaires étrangères et Commerce

27-28 mars 2013 : Le directeur exécutif a assisté à la conférence sur l'Échange de la gouvernance publique à l'Institut sur la gouvernance publique à Ottawa.

6-8 février 2013 : Le directeur exécutif a participé à la 14^e conférence annuelle sur la confidentialité et la sécurité à Victoria, en Colombie-Britannique.

22 janvier 2013 : Le directeur exécutif a rencontré, lors d'une réunion de suivi, les membres de la délégation française parlementaire dédiée au contrôle de la communauté du renseignement à Ottawa.

19-20 novembre 2012 : Le président du CSARS et les membres du Comité se sont déplacés dans les bureaux régionaux du SCRS en Colombie-Britannique et dans les Prairies.

11 octobre 2012 : La directrice exécutive du CSARS a rencontré une délégation du gouvernement français à Ottawa, notamment le coordonnateur national du renseignement.

19-20 novembre 2012 : Le président du CSARS et les membres du Comité se sont déplacés dans les bureaux régionaux du SCRS en Colombie-Britannique et dans les Prairies.

22 janvier 2013 : Le directeur exécutif a rencontré, lors d'une réunion de suivi, les membres de la délégation française parlementaire dédiée au contrôle de la communauté du renseignement à Ottawa.

6-8 février 2013 : Le directeur exécutif a participé à la 14^e conférence annuelle sur la confidentialité et la sécurité à Victoria, en Colombie-Britannique.

27-28 mars 2013 : Le directeur exécutif a assisté à la conférence sur l'Échange de la gouvernance publique à l'Institut sur la gouvernance publique à Ottawa.

SECTION 3

SURVOL DU CSARS

de la collectivité du renseignement. À ces échanges se greffent des entretiens avec des universitaires et des experts du renseignement et de la sécurité et d'autres organismes compétents. Ces activités enrichissent les connaissances du CSARS au sujet des questions et débats qui entourent le paysage de la sécurité nationale au Canada.

Les membres et les cadres du Comité visitent aussi les bureaux régionaux du SCRS afin de comprendre et d'évaluer le travail courant des enquêteurs locaux. Ces visites leur fournissent l'occasion de se faire exposer les problèmes, difficultés et priorités propres à ces bureaux par les cadres régionaux du Service. Elles leur permettent aussi de faire valoir ce qui polarise les efforts et les préoccupations du CSARS.

Au chapitre des ressources humaines, le CSARS continue de gérer ses activités dans les limites des ressources qui lui sont octroyées. Ses principales dépenses ont trait au traitement de son personnel et à ses déplacements afin de participer aux audiences, aux exposés et aux activités de surveillance du Comité au Canada.

COMPOSITION DU COMITÉ

Le CSARS est présidé par l'honorable Chuck Strahl, C.P. Les autres membres du Comité sont l'honorable Frances Lankin, C.P., C.M., l'honorable Denis Losier, C.P., C.M., l'honorable Deborah Grey, C.P., O.C., et l'honorable L. Yves Fortier, C.P., C.C., O.Q., c.r.

PERSONNEL ET ORGANISATION

Le CSARS jouit du soutien d'un directeur exécutif, Michael Doucet, et d'un effectif autorisé de 17 employés, en poste à Ottawa. Cet effectif comprend un directeur de la recherche, un avocat principal, un directeur des services généraux et d'autres professionnels et agents administratifs.

Le Comité dicte au personnel l'orientation à donner aux travaux de recherche et autres activités désignées prioritaires pour l'année. La marche des affaires courantes est confiée au directeur exécutif qui s'enquiert au besoin de la ligne de conduite à tenir auprès du président, en sa qualité de premier dirigeant du CSARS.

Dans le cadre de leurs travaux suivis, le président et les membres ainsi que les cadres supérieurs du Comité prennent part régulièrement à des discussions avec la direction et le personnel du SCRS et d'autres membres

Toutefois, le Comité a constaté qu'il y avait des retards et des périodes d'inactivité dans le dossier qui, cumulés, ont rendu le délai global déraisonnable. Le CSARS a réitéré l'une de ses recommandations pour qu'un système de suivi soit mis en place, et ce, afin d'identifier les dossiers qui dépassent le temps moyen de traitement pour que priorité leur soit donnée. De plus, le CSARS recommande que des systèmes de gestion du temps et des rappels soient mis en œuvre pour éviter de telles situations.

ENQUÊTE DU CSARS

RÉVOCATION D'HABILITATIONS DE SÉCURITÉ

Le CSARS a examiné séparément deux plaintes connexes en vertu de l'article 42 de la *Loi sur le SCRS* émises par des fonctionnaires dont les habilitations de sécurité avaient été révoquées sur la base de leur association avec une entité tierce.

Le Comité a constaté qu'il existait des motifs raisonnables de douter de la fiabilité des plaigants, et ce, en raison de relations avec des personnes ou des groupes soulevant des préoccupations. À cet égard, les plaigants pourraient agir ou être incités à agir de façon à constituer une menace envers la sécurité du Canada. Pour ces raisons, le CSARS recommande que la décision de révoquer les habilitations de sécurité des plaigants soit maintenue.

À la suite de ces enquêtes, le CSARS recommande également la révision de certaines lignes directrices de politiques pour les employés sur la question de ce qu'ils peuvent divulguer à des tiers en ce qui concerne l'identité de leur employeur, et a conseillé une politique plus cohérente définissant les situations où une telle divulgation est appropriée.

Le CSARS a constaté que, bien que les droits du plaigant n'aient pas été violés, l'employé du SCRS aurait dû faire preuve de souplesse pour tenir compte de certaines demandes du plaigant lors de l'entrevue. De même, le CSARS n'a trouvé aucune preuve de conduite répréhensible de la part de l'employé, mais il a noté que, dans un cas, il aurait pu être plus sensible aux craintes du plaigant. Le CSARS a rappelé au Service que ses employés devaient faire preuve d'ouverture lors d'entretiens avec des personnes qui viennent de pays où les services de renseignement sont craints, et devaient éviter toute action qui pourrait être interprétée comme étant abusive ou manipulatrice.

Le Comité a aussi constaté que l'employé du SCRS avait été bien préparé avant l'entrevue, et qu'il avait une connaissance suffisante de la culture et du pays du plaigant. Enfin, le CSARS recommande qu'au lieu d'éviter de reporter les entrevues d'immigration et de causer des retards supplémentaires excessifs, le SCRS émette une directive opérationnelle à tous les bureaux régionaux, conformément avec l'orientation prise par la région de Toronto, selon laquelle les enquêteurs sont tenus d'amener des appareils d'enregistrement à toutes les entrevues d'immigration et de veiller à ce qu'ils soient en état de marche.

ALLÉGATIONS DE RETARD À FOURNIR UNE ÉVALUATION DE SÉCURITÉ

ENQUÊTE DU CSARS

Le CSARS a enquêté sur une plainte en vertu de l'article 41 de la *Loi sur le SCRS* à l'égard d'une allégation de retard du SCRS à fournir une évaluation de sécurité en vue d'une habilitation d'accès au site du plaigant. Le plaigant a fait valoir que le retard lui avait fait perdre des possibilités d'emploi. Le Comité a constaté que le processus suivi par le Service, ainsi que les décisions et mesures prises dans le cadre de l'évaluation, avaient été raisonnables. L'agent chargé du dossier et l'enquêteur ont fait une enquête minutieuse pour s'assurer que l'évaluation était juste.

ethnique, et ce, comme un moyen possible de rassurer le public sur le fait que le SCRS ne fait pas de profilage racial.

Le CSARS a constaté qu'il n'y avait pas eu d'atteinte à la liberté de religion dans le contexte du processus d'évaluation de l'habilitation de sécurité du gouvernement, et que l'enquête du SCRS se justifiait dans le cadre de la politique de filtrage de sécurité en vigueur. Le CSARS a conclu que l'allégation de retard injustifié était sans fondement.

Le CSARS n'a pas trouvé que le SCRS avait communiqué des informations trompeuses au sujet du plaignant. Cependant, le Comité a constaté que les informations fournies à l'autre ministère du gouvernement étaient incomplètes, car certaines des conclusions de l'évaluation avaient été exclues. Le CSARS recommande que le SCRS remédie à la situation en envoyant les informations précédemment exclues au ministère concerné.

Enfin, le plaignant a également allégué qu'il existait dans l'autre ministère concerné de nombreux exemples de profilage dans des documents internes le concernant, et ce, après que le Service ait partagé de l'information, que ce même ministère n'avait pas officiellement refusé sa demande d'habilitation de sécurité, l'empêchant ainsi de trouver un recours en vertu de l'article 42 de la *Loi sur le SCRS*. En raison des limites du mandat du CSARS dans cette enquête en vertu de l'article 41 de la *Loi sur le SCRS*, le Comité n'a pas été en mesure de tirer des conclusions sur cette question.

ENQUÊTE DU CSARS

ALLÉGATIONS DE REFUS DES DROITS FONDAMENTAUX ET DE CONNAISSANCES CULTURELLES INSUFFISANTES DE LA PART DU SCRS

Le CSARS a enquêté sur une plainte en vertu de l'article 41 de la *Loi sur le SCRS* relative à la conduite d'un employé du SCRS lors d'une entrevue de pré-sélection dans le cadre d'une demande de résidence permanente. Le plaignant a allégué que l'employé du SCRS lui avait refusé certains droits fondamentaux, s'était comporté de façon inappropriée, et n'avait pas une connaissance suffisante de son pays d'origine et du contexte culturel de celui-ci.

ENQUÊTE DU CSARS

ALLÉGATIONS DE HARCÈLEMENT, DE PROFILAGE RACIAL ET DE PARTAGE DE DONNÉES TROMPEUSES

Le CSARS a enquêté sur une plainte en vertu de l'article 41 de la *Loi sur le SCRS*, dans laquelle le plaignant a allégué qu'un employé du SCRS, lors d'une entrevue avec lui, s'était comporté d'une manière qui constituait du harcèlement, qu'il avait utilisé des stratégies d'entrevue inappropriées, avait proféré des menaces, et avait menti au sujet de l'impact de l'entrevue sur l'habilitation de sécurité du plaignant. Il a également allégué que le SCRS faisait du profilage racial et que d'autres employés du Service avaient porté atteinte à sa liberté de religion au cours d'entretiens dans le cadre du processus d'évaluation en vue d'une habilitation de sécurité du gouvernement. Enfin, le plaignant a allégué que l'enquête du SCRS relative à l'évaluation de son habilitation de sécurité avait été insuffisante, avait conduit au partage de données trompeuses sur lui avec un ministère du gouvernement, et que le processus avait subi des retards abusifs.

Le CSARS a conclu que la conduite du premier employé du Service ne constituait pas du harcèlement et qu'il n'avait pas employé de stratégies inappropriées, mais que son choix de sujets et le ton de la discussion avaient créé des tensions inutiles lors de l'entrevue. Il a aussi constaté que la conduite de l'employé avait été trompeuse, car celui-ci a profité du processus d'habilitation de sécurité pour soustraire des informations au plaignant. Le CSARS a recommandé au SCRS d'aborder la question au niveau opérationnel et politique afin de réduire le risque qu'un tel scénario se reproduise.

Le CSARS a constaté qu'il n'y avait aucune preuve de profilage racial dans ce cas, et que le Service était dans son plein droit de conduire une telle enquête de sécurité sur le plaignant, et ce, sur la base de l'information dont il disposait pour s'acquitter de son mandat. Néanmoins, le CSARS a également constaté qu'il n'est pas déraisonnable, pour les personnes comme le plaignant qui n'ont pas accès à des informations classifiées, de se sentir ciblées. À cet égard, le CSARS recommande au SCRS de communiquer avec les communautés minoritaires pour aborder la question de la collecte des données concernant l'origine

Le tableau 1 expose l'état des diverses plaintes qui ont été présentées au CSARS au cours des trois derniers exercices financiers, y compris celles qui lui ont été adressées à tort, qui étaient hors de sa compétence ou qui ont été réglées à la suite d'une enquête sans audience (p. ex. par un examen administratif).

TABLEAU 1 : PLAINTES PRÉSENTÉES AU CSARS

Rapportées de l'exercice précédent			
Nouvelles plaintes			
Total	48	33	39
Dossiers réglés [†]	32	11	14

[†] Les dossiers réglés comprennent les plaintes qui ont donné lieu à un rapport, que le Comité a jugées hors de sa compétence, ou encore qui ne remplissent pas les conditions préliminaires ou ont été abandonnées.

CRITÈRES DE COMPÉTENCE DU CSARS À EXAMINER UNE PLAINTÉ...

... en vertu de l'article 41

En vertu de l'article 41 de la *Loi sur le SCRS*, le CSARS est tenu de faire enquête sur les plaintes que « toute personne » peut porter contre « des activités du Service ». Pour que le CSARS fasse enquête, deux conditions doivent être remplies :

1 le plaignant doit d'abord avoir présenté sa plainte par écrit au directeur du SCRS sans recevoir de réponse dans un délai raisonnable (environ 30 jours) ou, s'il en a reçu une, sans que cette réponse le satisfasse;

2 le CSARS doit être convaincu que la plainte n'est pas frivole, vexatoire ou sans objet, ni entachée de mauvaise foi.

Le CSARS ne peut enquêter sur une plainte qui peut être réglée autrement, par une procédure de griefs en vertu de la *Loi sur le SCRS* ou de la *Loi sur les relations de travail dans la fonction publique*.

... en vertu de l'article 42

Quant aux habilitations de sécurité, le CSARS est tenu, selon l'article 42 de la *Loi sur le SCRS*, de faire enquête sur les plaintes présentées par :
1 les personnes qui ne sont pas embauchées par le gouvernement fédéral à cause du refus d'une habilitation de sécurité;

2 les fonctionnaires fédéraux qui sont renvoyés, rétrogradés ou mutés ou qui se voient refuser une mutation ou une promotion pour la même raison;

3 les personnes qui se voient refuser un contrat pour la fourniture de biens ou de services au gouvernement, toujours pour le même motif.

Les plaintes semblables doivent être présentées dans les 30 jours du refus de l'habilitation de sécurité. Le CSARS peut prolonger cette période si des raisons valables lui sont fournies.

B. PLAINTES

Outre sa fonction de surveillance, le CSARS est investi de celle d'enquêter sur les plaintes présentées par des personnes ou des groupes à l'endroit du SCRS. Les types de plaintes visées par ses enquêtes sont décrits dans la *Loi sur le SCRS* et peuvent prendre diverses formes, dont deux sont plus fréquentes. En vertu de l'article 41 de la *Loi sur le SCRS*, le CSARS enquête sur les plaintes qui concernent « des activités du Service ». Selon l'article 42, il enquête sur celles qui ont trait au refus d'habilitations de sécurité à des fonctionnaires ou à des fournisseurs du gouvernement fédéral. Beaucoup moins souvent, le CSARS fait enquête sur des renvois de la Commission canadienne des droits de la personne ou sur des rapports du ministre concernant la *Loi sur la citoyenneté*.

Le processus relatif aux plaintes au CSARS

La première étape d'un dossier de plainte peut être la présentation d'une demande de renseignements au CSARS, soit par écrit, en personne ou par téléphone. Sur réception d'une plainte écrite, le personnel du CSARS informe le plaignant éventuel des exigences de la *Loi sur le SCRS*, afin de pouvoir ouvrir un dossier de plainte officiel.

Lorsqu'il reçoit une plainte officielle par écrit, le CSARS effectue un examen préliminaire. Celui-ci peut porter sur toute information que peut détenir le SCRS, à l'exception des documents confidentiels du Cabinet. Si la plainte ne satisfait pas à certaines exigences de la loi, le CSARS la déclare hors de sa compétence et n'ouvre pas d'enquête à ce sujet.

Si le CSARS détermine qu'il a compétence, il enquête sur la plainte lors d'une audience quasi judiciaire, présidée par un ou plusieurs de ses membres que secondent son personnel et son équipe de juristes en leur fournissant des avis concernant la procédure et les questions de fond.

Des rencontres peuvent être tenues avec les parties, avant l'audience, pour établir et arrêter les questions sur préliminaires de procédure, comme les allégations sur lesquelles faire enquête, la forme à donner à l'audience,

L'identité et le nombre des témoins à citer, les documents à préparer en vue de l'audience ainsi que la date et l'endroit de celle-ci.

Le temps nécessaire à l'enquête et au règlement d'une plainte peut varier d'après divers facteurs, dont la complexité du dossier, la quantité de documents à examiner, le nombre de jours d'audience requis (tant en présence qu'en l'absence du plaignant) et la disponibilité des participants.

Selon la *Loi sur le SCRS*, les audiences du CSARS doivent être tenues « en secret ». Chacune des parties a le droit d'être représentée par un avocat et de formuler des observations à l'audience, mais aucune ne peut, de plein droit, être présente au moment où une autre personne expose ses observations au CSARS, ni y avoir accès ou les commenter.

Une partie peut demander une audience *ex parte* (en l'absence du plaignant et, peut-être, d'autres parties) au cours de laquelle elle présente des preuves qui, pour des raisons de sécurité nationale ou pour d'autres motifs que le CSARS juge valables, ne peuvent être révélées à l'autre partie ou à son avocat. Lors d'une telle audience, l'équipe de juristes du CSARS contre-interroge les témoins pour s'assurer que les preuves ont été bien vérifiées et sont fiables. Cela permet de fournir au membre-président l'information factuelle complète et exacte en tous points au sujet de la plainte.

Une fois clos le volet *ex parte* de l'audience, le CSARS détermine si l'essentiel de la preuve peut être dévoilé aux parties exclues. Le cas échéant, il prépare un résumé de la preuve et le leur présente, une fois celui-ci expurgé pour des raisons de sécurité nationale.

Après avoir terminé son enquête sur une plainte portée en vertu de l'article 41, le CSARS présente un rapport au directeur du SCRS et au ministre de la Sécurité publique ainsi qu'une version déclassifiée du rapport au plaignant. Dans le cas d'une plainte déposée en vertu de l'article 42, le CSARS remet aussi son rapport à l'administrateur général compétent.

du SCRS, notamment des statistiques sur les activités de base du Service, telles que les opérations de ciblage, es opérations qui font appel à des sources humaines et les demandes de mandat, ainsi que des informations sur les activités de liaison au Canada et à l'étranger, l'appui technique et opérationnel, les opérations à l'étranger et les filtres de sécurité. Les réponses du Service ont permis au CSARS de dresser un portrait complet de l'étendue de ses activités, et le Comité a ainsi pu évaluer le rapport du directeur dans son ensemble.

Le CSARS a constaté que le rapport du directeur offrait un aperçu utile et complet de l'ensemble des opérations du SCRS. Néanmoins, le Comité a trouvé qu'il ne contenait pas de description détaillée des activités du Service conformément à l'article 16, « assistance ». Ces activités font partie intégrante des opérations du Service, et le CSARS estime qu'une description plus détaillée est justifiée.

Le Comité a également constaté que le rapport du directeur ne décrivait pas suffisamment les activités à l'étranger du Service. Il estime que des informations plus détaillées auraient fourni une description plus précise et plus représentative des opérations à l'étranger du Service, et aideraient le ministre à mieux comprendre le degré élevé de menace qui pèse sur la vie des employés travaillant dans ces milieux. Le directeur du SCRS pourrait envisager d'inclure cette information dans le rapport de l'année prochaine, et le CSARS estime que cette question est suffisamment importante pour mériter l'attention du ministre et un examen continu.

Respect de la Loi sur le SCRS, des directives ministérielles, et de l'exercice des pouvoirs du Service

Le Comité doit indiquer si le rapport du directeur lui paraît acceptable, et si, à son avis et en vertu de l'article 38 (2) de la *Loi sur le SCRS*, les activités opérationnelles visées dans le rapport ne sont pas autorisées sous le régime de la *Loi* ou des instructions données par le ministre ou comportent un exercice abusif ou inutile par le Service de ses pouvoirs.

À cette fin, le CSARS a passé en revue le contexte de l'examen, notamment les récentes modifications apportées à la *Loi sur le SCRS*, le pouvoir du Service de recueillir des renseignements en vertu de l'article

16, les directives ministérielles pertinentes et les priorités en matière de renseignement. Le Comité a également examiné le cadre de gouvernance interne du Service, notamment les directives internes et les politiques opérationnelles.

Le CSARS a constaté qu'à une exception près, la structure de gouvernance interne du Service respectait la *Loi sur le SCRS* et les directives ministérielles. Le Comité a conclu que la pratique du Service de partager de l'information avec les organisations du renseignement d'origine électromagnétique canadiennes et étrangères était potentiellement problématique en termes de conformité avec les directives ministérielles sur le partage de l'information. Ce problème n'est pas uniquement apparu au cours du processus de remise du certificat, il a été noté dans le cadre d'une étude du CSARS intitulée « Les relations et échanges du SCRS avec le Centre de la sécurité des télécommunications Canada (CSTC) » qui s'est penchée sur la question au cours de la période visée par le rapport du directeur 2011-2012. Aux fins de la certification du rapport du directeur, le CSARS ne considère pas cette question comme un cas de non-respect des directives ministérielles. Néanmoins, le CSARS estime que la situation est suffisamment préoccupante pour que le ministre en tienne compte.

À l'exception d'un domaine, le Comité estime que les activités, telles qu'elles sont décrites dans le rapport, sont conformes à la *Loi* et aux directives ministérielles, et constituent un exercice raisonnable et nécessaire des pouvoirs du Service. Plus précisément, le Comité a déterminé que les activités décrites dans le rapport étaient compatibles avec les obligations et fonctions énoncées dans les articles 12 à 20 de la *Loi sur le SCRS* et, en vertu de l'article 16, se conformaient aux demandes du ministre des Affaires étrangères et du ministre de la Défense nationale, ainsi qu'aux directives ministérielles sur les opérations, le partage de l'information et les priorités en matière de renseignement.

REMISE DU CERTIFICAT AU RAPPORT ANNUEL DU DIRECTEUR DU SCRS AU MINISTRE DE LA SÉCURITÉ PUBLIQUE : SURVOL

Conformément aux nouvelles exigences réglementaires, le CSARS a remis un certificat au rapport annuel du directeur du SCRS au ministre de la Sécurité publique. L'énoncé de l'article 38 (2) de la *Loi sur le SCRS* traite de garanties importantes quant à la légalité, la nécessité et le caractère raisonnable des activités opérationnelles du Service. Par ailleurs, le rapport du directeur a dressé, ces dernières années, un aperçu utile et complet de l'ensemble des opérations du SCRS. Le rapport pour l'exercice 2011-2012 n'a pas déroge à la règle, et a fourni un résumé des principales réalisations du Service au cours de l'année passée, ainsi que des défis opérationnels rencontrés. Par conséquent, pour le CSARS la remise du certificat aux « activités opérationnelles décrites dans le rapport » revenait à remettre un certificat à la quasi-totalité des activités du SCRS pour l'exercice 2011-2012.

À l'exception de trois points, le Comité s'est montré satisfait du rapport du directeur sur les activités opérationnelles du Service pour la période visée 2011-2012. En outre, il estime que les activités opérationnelles, telles qu'elles sont décrites dans le rapport du directeur, ne contreviennent pas à la *Loi sur le SCRS* ou aux directives ministérielles, et qu'elles ne comportent pas un exercice abusif ou inutile par le Service de ses pouvoirs.

Satisfaction du CSARS à l'égard du rapport

Le rapport du directeur, présenté en application de l'article 6 (4) de la *Loi sur le SCRS*, vise à fournir au ministre des informations pour l'aider dans l'exercice de sa responsabilité ministérielle à l'égard du SCRS. Le CSARS se montre satisfait du rapport du directeur si celui-ci remplit cette fonction, et ce, en fonction de trois critères : premièrement, si le rapport satisfait aux exigences des instructions du ministre énoncées dans les Directives ministérielles de 2008 sur les opérations et aux Directives ministérielles sur les priorités de renseignement de 2011-2012; deuxièmement, si les faits contenus dans le rapport sont exacts; et, troisièmement, si, de l'avis du CSARS, le rapport offre une représentation exacte des activités du SCRS au cours de l'exercice 2011-2012.

Le CSARS a constaté que le rapport du directeur répondait à toutes ces exigences, sauf une. Pendant le processus de remise du certificat, le CSARS a appris que, même si le point en question n'avait pas été traité dans le rapport, le Service avait fourni au ministre l'information dans le cadre d'un mémoire au Cabinet. Cette omission n'a donc pas influé sur la satisfaction globale du CSARS à l'égard du rapport du directeur. En ce qui concerne l'exactitude du rapport du directeur, le Comité estime que les informations fournies sont, dans l'ensemble, factuelles. Le CSARS a examiné les énoncés du rapport, les a comparés aux informations détenues par le Service et, lorsque cela s'est avéré nécessaire, le Comité a présenté des demandes écrites pour obtenir des documents et des éclaircissements supplémentaires. Sur la base de cet examen, le Comité a déterminé qu'à l'exception de deux énoncés, le rapport du directeur était étayé et documenté de façon appropriée. Les erreurs relevées étaient liées à la désignation précise de l'état de la relation du Service avec une autre organisation et à l'omission d'une opération du nombre total de ces types d'opérations.

Le CSARS a examiné le rapport du directeur pour voir s'il offrait une représentation exacte des activités du SCRS au cours de la période visée 2011-2012. À cette fin, le Comité a présenté des demandes écrites de renseignements sur les activités opérationnelles

MODIFICATIONS APPORTÉES À LA LOI SUR LE SCRS

En 2012, le gouvernement du Canada a modifié la *Loi sur le SCRS* pour que le CSARS endosse certaines des responsabilités autrefois confiées à l'inspecteur général du Service. L'une des responsabilités majeures concerne l'exigence que le CSARS remette au ministre de la Sécurité publique un certificat indiquant dans quelle mesure le rapport lui paraît acceptable. En outre, le Comité signale toute activité opérationnelle du Service visée dans le rapport qui, selon lui, n'est pas autorisée sous le régime de la *Loi sur le SCRS* contrevient aux instructions données par le ministre émises en vertu de la *Loi* ou comporte un exercice abusif ou inutile par le Service de ses pouvoirs.

Globalement, les points ci-dessus et d'autres recommandations du CSARS ont fondamentalement changé la façon dont le SCRS exerce ses activités, notamment en matière de mise en œuvre de nouvelles directives ministérielles et politiques en matière de collecte, de conserve, d'analyse et de transmission de renseignements du Service, ainsi que dans la manière dont les relations du Service avec les organismes ministériels nationaux et étrangers devraient être gérés. Par conséquent, le programme opérationnel entier du SCRS, au Canada et surtout à l'étranger, ne ressemble en rien à celui examiné dans les années sur lesquelles porte l'étude.

Il est peut-être tout aussi important de noter que l'affaire Abdelrazik a gagné en ampleur et en complexité au fil des années. Tandis que l'enquête du SCRS se tarissait de manière significative (compte tenu de l'incapacité indéterminée apparente de M. Abdelrazik à quitter le Soudan), d'autres ministères du gouvernement du Canada, notamment le MAECI, la GRC, l'ASFC et Transports Canada (ainsi que des organismes gouvernementaux étrangers) commençaient à se batailler sur son sort. Le CSARS ne peut déterminer dans quelle mesure ces entités ont pu agir sur la base de conseils du SCRS, ou dans quelle mesure l'information du SCRS a joué dans la prise de décision. En effet, le mandat du Comité se limite au SCRS et, par conséquent, il a dû se borner à commenter les faits relatifs à l'implication du Service dans l'affaire.

Conclusions

Pour toutes ces raisons, le CSARS a choisi de ne pas émettre de recommandations en matière de politique ou de pratique dans le cadre de cette étude. En effet, la plupart des politiques du Service pertinentes ont déjà changé, et/ou les pratiques opérationnelles ont évolué au cours des dix dernières années. Toute recommandation du CSARS aurait été déjà faite par des commissions d'enquête, les décisions des tribunaux canadiens, ou par le Comité lui-même.

Le Comité estime néanmoins qu'un certain nombre de précieuses leçons peuvent être tirées de l'étude du CSARS sur le rôle du SCRS dans l'affaire Abdelrazik. Il est préoccupant que le SCRS ait élaboré des évaluations des menaces fondées sur des informations inexactes et exagérées, et que des informations classifiées aient été traitées de façon inappropriée, en dépit

de la politique actuelle et l'orientation spécifique en la matière de la haute gestion. Toutes aussi inquiétantes sont les relations du SCRS avec ses partenaires du gouvernement du Canada, en particulier, dans le cas présent, le MAECI.

Comme le CSARS a souligné dans une série d'études récentes (dans lesquelles figurent certaines des recommandations pertinentes citées ci-dessus), le SCRS est en pleine expansion à l'étranger, et les partenariats du Service avec d'autres grandes organisations gouvernementales sont de plus en plus fréquents, et de plus en plus intégrés. Cependant, le SCRS devra faire face à des responsabilités et des attentes plus grandes dans ce rôle. Par exemple, en 2012, le SCRS a dit au CSARS que la législation et les protocoles existants « permettent, mais ne nécessitent pas » que le Service partage une information qui serait d'une importance cruciale pour le travail de partenaires gouvernementaux. Cette affirmation est techniquement correcte, mais une telle approche réduit ou sape toute intention de favoriser des relations de travail plus étroites et plus intégrées entre les organismes gouvernementaux. Le CSARS encourage fortement le SCRS à voir ce rapport comme une rétrospective détaillée, et une occasion de réévaluer sa posture et sa démarche visant à faire partie d'une approche pangouvernementale.

Enfin, cette étude a dû se réduire aux activités du SCRS, limite que le Comité a déjà publiquement commentée. Bien que le Comité spécial du sénat qui, en 1984, a examiné le projet de loi qui allait devenir la *Loi sur le SCRS*, ait entrevu « l'importance vitale du rôle que le CSARS serait appelé à jouer dans le cadre du système de renseignement de sécurité », en veillant au besoin « à ce que certaines questions touchant la sécurité fassent l'objet d'un débat adéquat », cette fonction se heurte aux limites pratiques de notre mandat.

Par conséquent, même si nous sommes confiants dans notre étude du rôle du SCRS dans l'affaire Abdelrazik, elle ne peint pas un tableau complet ou définitif du sujet. D'autres informations peuvent resurgir de tout l'éventail de documents ou de rapports que d'autres ministères et organisations du Canada, également impliqués, ont en main, ainsi que des procédures judiciaires en cours. À l'heure actuelle, la page n'est pas encore complètement tournée sur l'affaire Abdelrazik.

à l'affaire Abdelrazik. Le CSARS a notamment recommandé que :

- Dans la collecte d'information, le SCRS évite de faire de longs rapports sur des individus non ciblés (cf. Rapport annuel 2002-2003 : Menaces intérieures et défense de causes, protestations, manifestation de désaccords);
- Le SCRS élabore une politique opérationnelle concernant la documentation de ses relations avec les organismes qui sont connus pour leurs violations des droits de la personne ou auxquels on attribue de tels gestes (cf. Rapport annuel 2005-2006 : Liaison du SCRS avec des organismes étrangers : examen d'un bureau de liaison-sécurité);
- Le SCRS examine son utilisation des techniques d'enquête afin qu'elles reflètent les pratiques exemplaires actuelles (cf. Rapport annuel 2005-2006 : Examen des techniques de surveillance électro-nique et de collecte d'information du SCRS);
- Le protocole d'entente conclu entre le SCRS et le MAECI soit mis à jour et désigne ce ministère à titre d'organisme principal dans les affaires de citoyens canadiens détenus à l'étranger. Le protocole devrait aussi refléter celui recommandé par le juge O'Connor, à savoir « des consultations franches et à point nommé entre les organismes canadiens » qui peuvent avoir un rôle à jouer à l'égard des Canadiens détenus à l'étranger, « une démarche cohérente et unifiée » menée par le MAECI et « la reddition de comptes à l'égard des mesures adoptées » en pareil cas (cf. Rapport annuel 2006-2007 : Étude de l'affaire Mohammed Mansour Jabarah);
- Le SCRS instaure des mesures pour intégrer dans son travail courant les valeurs découlant des faits récents sur la scène politique, judiciaire et juridique, afin de maintenir sa propre crédibilité et de combler les attentes croissantes et changeantes quant aux modalités d'opération et de rendement d'un service de renseignement dans une société démocratique contemporaine (cf. Rapport annuel 2008-2009 : Rôle joué par le SCRS dans l'affaire Omar Khadr);
- Le SCRS adopte une interprétation plus large de son engagement à communiquer des renseignements au MAECI (cf. Rapport annuel 2010-2011 : La relation du SCRS avec un partenaire des « Five Eyes »).

quitte le Soudan (atténuant ainsi l'impact de ce que les évaluations affirmaient), le CSARS a constaté que ces évaluations étaient exagérées et transmettaient des informations inexactes.

Enfin, le CSARS avait des préoccupations à l'égard de l'enquête du SCRS, et notamment sur le fait que le Service avait produit des rapports de façon excessive, et donc avait gardé dans ses bases de données opérationnelles une quantité importante d'informations non liées à la menace, et provenant de personnes qui n'étaient pas des cibles.

Préparation du rapport du CSARS

Le CSARS a constaté qu'il était difficile de replacer les conclusions de cette étude dans le contexte. Prés de dix ans se sont écoulés depuis que M. Abdelrazik a quitté le Canada pour le Soudan, et c'est un euphémisme de noter que depuis les événements de 2003 et de 2004, beaucoup de choses ont changé dans le domaine de la sécurité et du renseignement au Canada.

Tout d'abord, plusieurs commissions d'enquête canadiennes, notamment les rapports des commissions d'enquête O'Connor (2006), Iacobucci (2008) et Major (2010) ont largement fait état de tout un éventail de questions liées à la sécurité et au renseignement. Bien que n'étant pas directement liées à l'affaire Abdelrazik, les nombreuses recommandations issues de ces enquêtes visaient à améliorer les normes professionnelles attendues de la part des ministères et agences du gouvernement impliqués dans des questions de sécurité et de renseignement, et dans de nombreux cas, visaient en particulier à améliorer les pratiques du SCRS.

Il faut également prendre en considération toute la jurisprudence élaborée au cours des dix dernières années et qui traite des rôles et des responsabilités du ou des gouvernements, des citoyens et des résidents permanents quand la question de la sécurité nationale est au cœur du débat. Le difficile cheminement de M. Abdelrazik au cœur du système judiciaire canadien a été très médiatisé, nul n'est besoin d'en refaire ici état. De son côté, le CSARS n'a pas été un simple spectateur passif durant cette tumultueuse décennie. En fait, beaucoup des recommandations antérieures du Comité concernent des questions qui se rapportent

Méthode

Le CSARS a demandé au SCRS toutes les informations pertinentes concernant M. Abdelrazik lors de la période sur laquelle portait l'étude, notamment les rapports opérationnels, la correspondance interne et les informations relatives aux échanges du SCRS avec des partenaires canadiens et étrangers. Après examen des documents, le CSARS a posé des questions pour éclaircir un certain nombre de points, et demandé à parler à certaines personnes clés directement impliquées dans l'enquête et le traitement de cette affaire.

Durant l'étude, le SCRS a informé le CSARS de préoccupations d'ordre juridiques, car l'étude du Comité a pris place en même temps que la procédure de M. Abdelrazik contre le gouvernement canadien. Par conséquent, le CSARS n'a pu avoir accès au personnel concerné qu'avec beaucoup de retard. En outre, le SCRS n'a au début répondu qu'à une partie des questions écrites du Comité et, dans un certain nombre de cas, ses réponses n'étaient pas complètes. Après des délibérations et des consultations poussées à l'interne, il a été réitéré au SCRS que les activités faisant partie du mandat du CSARS et les procédures judiciaires en cours étaient deux processus distincts et séparés, et que l'un n'entravait pas les progrès de l'autre.

Le CSARS a fini par recevoir des réponses complètes et bénéficier de la pleine coopération du Service. Le Comité a aussi finalement pu s'entretenir avec plusieurs des personnes clés impliquées dans l'affaire, même si compte tenu du laps de temps écoulé depuis les événements, certaines ne travaillaient plus pour le Service. Compte tenu des retards que le Comité a rencontrés, il a choisi de restreindre l'objectif principal de l'étude et de s'intéresser principalement à la première phase de l'affaire, soit de mars 2003 à décembre 2004, durant la période dans laquelle le SCRS a été le plus impliqué. Après cela, l'affaire Abdelrazik est devenue beaucoup plus complexe, et un certain nombre d'autres organismes canadiens ont commencé à jouer des rôles importants dans celle-ci. En raison de la nature même de l'affaire et de la demande directe et publique de l'ancien directeur du SCRS, le Comité a décidé de soumettre son rapport directement au ministre de la Sécurité publique en vertu de l'article 54 de la *Loi sur le SCRS*.

Conclusions

Le CSARS a conclu que rien ne permettait de croire que le SCRS avait demandé aux autorités soudanaises d'arrêter ou de détenir M. Abdelrazik. Cependant, dans les mois qui ont précédé le départ pour l'étranger de M. Abdelrazik et son arrestation, le SCRS a tenu ses alliés du renseignement étrangers au courant de toute nouvelle information recueillie sur M. Abdelrazik.

Au cours du développement de l'affaire, le CSARS a conclu que les autorités soudanaises avaient gardé l'impression erronée que le Canada, notamment le SCRS, avait soutenu la décision initiale d'arrêter et de détenir M. Abdelrazik. Cette confusion pourrait s'expliquer par le fait que le noyau de cette affaire a été mis en avant comme une question liée aux renseignements, et il en est resté ainsi (selon les rapports) dans l'esprit des Soudanais. Pour compliquer encore plus les choses, à l'origine, les deux organisations gouvernementales les plus fortement impliquées dans l'affaire, le MAECI et le SCRS, ont mené respectivement leur travail consulaire et de renseignement en même temps, et parfois en contradiction. L'étude du CSARS a conclu que, quand le SCRS a appris que M. Abdelrazik était détenu au Soudan, le Service aurait dû se montrer plus transparent avec le MAECI au sujet de ce qu'il savait, et ce, afin d'assurer une réponse plus éclairée et coordonnée du Canada dans l'affaire.

L'étude du CSARS a soulevé un certain nombre de préoccupations. Tout d'abord, après l'incarcération initiale de M. Abdelrazik, le SCRS a été autorisé à s'entretenir avec lui au Soudan. Le Service a respecté les autorités compétentes en la matière en demandant leur approbation pour mener cet entretien. Toutefois, le CSARS a constaté que dans le cadre de son entretien et du rapport subséquent, le Service avait communiqué des informations personnelles et classifiées, et ce, de façon inappropriée et en manquant de sa politique.

Deuxièmement, au début de l'été 2004, et en préparation à la libération possible de M. Abdelrazik, le SCRS a mis au courant ses partenaires gouvernementaux des informations qu'il possédait. Cette mise à jour n'a pas été le dernier mot du Service en ce qui concerne son évaluation de la situation, et bien que cela ait pris des années avant que M. Abdelrazik

Le SCRS a fait bien des progrès dans l'utilisation de méthodes clandestines depuis la création du Service en 1984. En effet, l'une des pierres angulaires du succès de toute agence de renseignement est de mener ses opérations sans être observée. Le SCRS ne pourrait pas fonctionner efficacement sans avoir recours à des méthodes clandestines. Le Service prend des mesures novatrices pour améliorer la sécurité de ses diverses activités au Canada et à l'étranger, et de nouveaux défis ne manqueront pas de surgir. Le Comité se penchera donc sur d'autres aspects des méthodes clandestines du SCRS dans de futures études.

ÉTUDE DU CSARS LE RÔLE DU SCRS DANS L'AFFAIRE ABDELRAZIK

Contexte

Aboushan Abdelrazik, qui possède la double nationalité soudanaise et canadienne, a été arrêté par les autorités soudanaises en septembre 2003. Il est resté en exil au Soudan pendant six ans sans pouvoir rentrer au Canada. Début 2009, les médias canadiens ont déclaré que son arrestation et sa détention avaient été demandées par des agents du renseignement de sécurité du Canada, une accusation que le SCRS a toujours niée. Suite à ces allégations, le directeur du SCRS s'est adressé publiquement au président du CSARS, pour demander au Comité d'enquêter sur l'exécution des obligations et fonctions du Service dans cette affaire, et de dresser un rapport.

Au printemps de 2011, le CSARS a entrepris une étude pour examiner la participation du SCRS dans l'affaire Abdelrazik, et ce, pour la période allant des mois précédents le départ de M. Abdelrazik pour le Soudan en mars 2003 à son retour au Canada. Le Comité s'est intéressé à l'enquête du SCRS sur M. Abdelrazik et sur ses interactions avec lui au Canada et à l'étranger, et notamment sur le rôle que le Service aurait pu jouer dans son arrestation et sa détention par les autorités soudanaises. Il a également examiné les informations que le SCRS a reçues de partenaires canadiens et étrangers, ou qu'il leur a transmises, sur M. Abdelrazik. Plus largement, le CSARS a examiné le rôle et les conseils du SCRS dans l'approche « pangouvernementale » qui a finalement été utilisée dans cette affaire.

de données centralisée, et la formation d'une unité spécifique qui agit en tant que « centre des politiques » dans l'utilisation de la méthode. Un certain nombre de défis liés à la responsabilité financière se posaient avant l'audit interne du SCRS. Le CSARS a constaté que des exigences supplémentaires en matière de rapports financiers avaient été mises en place, et que d'autres améliorations étaient en cours.

Le SCRS a informé le Comité qu'au cours de la période sur laquelle l'étude porte, aucun cas où un employé du Service a été reconnu coupable d'un manquement à la sécurité et/ou impliqué dans une infraction à la sécurité liée à l'utilisation de cette méthode ne s'est présentée. Toutefois, le Comité a noté que, dans un cas au cours des dernières années, la sécurité de la méthode avait été compromise, mais que l'affaire avait été de nature procédurale/administrative et qu'elle n'avait pas causé de préjudice ou de risques importants. Les principaux intéressés à l'interne ont géré le problème, et les détails de l'affaire ont été classés dans un dossier, conformément à la politique du SCRS. Ici, bien que le Comité se soit montré globalement satisfait de la façon dont le problème a été traité, il a constaté l'absence de procédure établie exigeant que les autres régions du SCRS soient rapidement informées des leçons apprises à la suite d'une infraction de sécurité impliquant une méthode. Dans cette optique, le CSARS recommande que la politique du SCRS soit modifiée pour assurer que toutes les parties sont informées des leçons apprises à la suite d'une infraction de la sécurité suspectée ou confirmée concernant l'usage de cette méthode secrète.

Devant les préoccupations croissantes quant à la nécessité de mieux protéger les employés, les processus et les sources d'information du SCRS, l'usage de cette méthode est devenu de plus en plus fréquent. Pourtant, elle a créé divers problèmes de gestion, et l'un des plus pressants se trouve être la nécessité de maintenir les ressources humaines nécessaires pour assurer son utilisation efficace. L'une des solutions que le SCRS est en train d'élaborer est le recours à l'utilisation de matériel technique/d'un programme complémentaire pour aider à alléger cette charge de gestion. Bien que cette nouvelle initiative semble prometteuse, le CSARS a conclu que la politique de ce programme d'accompagnement était insuffisante, et qu'elle contredisait les principes d'autres politiques connexes. Le Comité recommande donc que le SCRS mette immédiatement à jour sa politique sur ce nouveau programme afin qu'elle soit plus en phase avec les autres politiques opérationnelles.



ÉTUDE DU CSARS

LE RECOURS DU SCRS AUX MÉTHODES CLANDESTINES

Contexte

Les méthodes clandestines (également souvent connues sous le nom « d'espionnage ») comprennent un large éventail de techniques spécifiques dont les risques sont mesurés, et donnent au Service les garanties de secret et de sécurité nécessaires pour l'assister dans ses tâches et fonctions. Les opérations du Service ont pris de l'ampleur, et ce, au Canada et à l'étranger, et les cibles ont des moyens de plus en plus perfectionnés. Le besoin s'est donc fait sentir d'améliorer les méthodes clandestines pour aider le Service à mieux protéger l'identité de ses employés, ses processus et ses sources d'information. Cette étude traite de l'une des méthodes spécialisées du SCRS.

Étude du CSARS

Le CSARS a examiné les documents pertinents et a parlé aux employés du SCRS responsables de l'élaboration, du traitement et de la logistique de cette méthode secrète. Les questions suivantes ont été abordées : les justifications de l'usage de cette méthode, les types de scénarios dans lesquels le Service y a recourus, le niveau de vérification, d'accès et de contrôle pour s'assurer que le matériel technique n'est pas utilisé à mauvais escient par les employés (et la satisfaction du CSARS en la matière) et, enfin, un examen des diverses relations que le SCRS doit maintenir pour assurer la gestion efficace de cette méthode.

La Direction de la vérification interne du SCRS avait déjà effectué une évaluation de cette méthode clandestine; l'un des objectifs supplémentaires du CSARS était donc d'examiner le niveau de réponse aux recommandations découlant de la vérification. Dans l'ensemble, notre étude a révélé que le Service y avait depuis apporté de nombreuses améliorations, notamment l'élaboration d'un cadre stratégique plus complet et d'un ensemble de lignes directrices pour mieux soutenir l'usage croissant de cette méthode secrète. Les bureaux régionaux du SCRS se partagent la responsabilité de l'usage de cette méthode. Cette approche donne aux gestionnaires régionaux la souplesse nécessaire pour recourir à la méthode en fonction de leurs besoins opérationnels, tout en laissant au siège un certain contrôle, notamment la création d'une base

communiquer sur ces menaces, quel que soit l'idéologie dont elles relèvent ou le groupe auquel elles appartiennent, et était plus logique et solide du point de vue de l'efficacité des recherches. Le Comité a aussi examiné certains dossiers et rapports opérationnels pour s'assurer que les enquêtes étaient menées de manière appropriée et raisonnable, c'est-à-dire dans le respect de la politique interne et du mandat du SCRS. Le CSARS a constaté que les activités liées uniquement à la protestation légitime et à la dissidence n'avaient pas été traitées, et que le Service avait mis fin aux rapports opérationnels sur plusieurs anciennes cibles. Le Comité a aussi noté que le SCRS avait rapidement mis un terme aux enquêtes sur les personnes qui n'étaient plus considérées comme des menaces après les grands événements 2010, et a encouragé le Service à faire preuve de vigilance à l'égard d'événements ou d'enjeux futurs.

Un défi demeure : le besoin inévitable du gouvernement d'obtenir des informations sur des menaces actuellement latentes, mais qui peuvent refaire surface rapidement. Le Service doit donc rester au courant des questions névralgiques ou des éléments déclencheurs possibles qui peuvent nourrir l'extrémisme intérieur et causer une menace à la sécurité nationale. En outre, en se tenant informé, le Service doit faire en sorte de ne pas empirer sur les formes légitimes de protestation. En fin de compte, ce sont les partenaires du Service avec les organismes d'application de la loi qui peuvent être la meilleure source d'information : les fonctionnaires chargés du maintien de l'ordre peuvent connaître des individus impliqués dans des activités criminelles, et qui sont susceptibles, à un moment donné, de constituer une menace selon le mandat du SCRS en matière d'enquête sur l'extrémisme intérieur. Certains partenaires avec les organismes d'application de la loi ont porté leurs fruits, tant dans des affaires où le Service ne menait plus d'enquête sur les anciennes menaces que dans de nouveaux domaines que le SCRS doit surveiller au cas où un lien avec une question de sécurité nationale se crée. Dans l'ensemble, le CSARS encourage l'orientation du Service en matière de liaison avec ses partenaires canadiens.

Cette étude s'est penchée sur le nouveau cadre du SCRS et les enquêtes effectuées après 2010. Aux fins de l'étude, le CSARS s'est déplacé dans un bureau régional dans lequel étaient menées des enquêtes actives liées à des activités extrémistes au Canada. Le CSARS souhaitait savoir comment les changements dans l'approche adoptée par le Service en matière d'extrémisme intérieur affectaient la stratégie nationale et les enquêtes locales. Le Comité a constaté que le nouveau cadre d'enquête récemment révisé dont le Service se sert désormais offre plus de souplesse pour collecter des renseignements et

Étude du CSARS

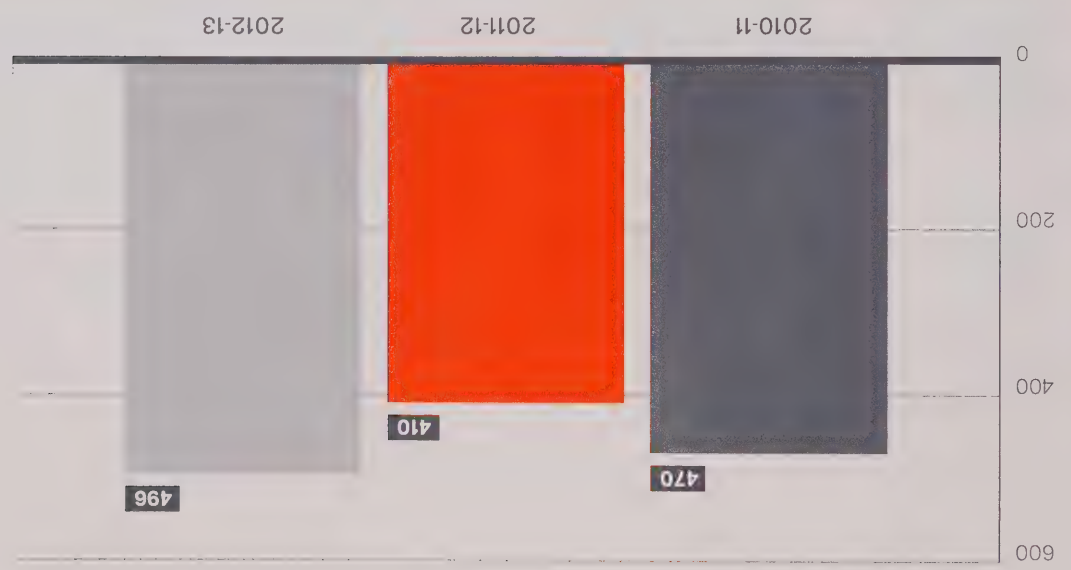
dernières années, le niveau de menace associé à un certain nombre de ces enquêtes internes a été réévalué, en particulier avec la clôture d'événements de grande envergure qui ont pris place en 2010 (par exemple, les Jeux olympiques et paralympiques de Vancouver, et les Sommits du G8 et du G20), autour desquels a gravité une violence ou des menaces accrues de violence temporaire. Le SCRS a donc apporté des changements à la façon dont il enquête sur l'extrémisme intérieur non religieux suite à la réévaluation de la menace.

Pour le SCRS, l'extrémisme intérieur se caractérise par la volonté d'individus ou de groupes, au Canada, d'utiliser la violence ou la menace de violence à des fins politiques et/ou idéologiques. Le SCRS consacre la plupart de ses ressources au contre-terrorisme à l'extrémisme religieux; cependant, il continue également à surveiller les individus et les organisations qui pourraient être impliqués dans d'autres formes de terrorisme, notamment dans des actes de violence liée à des questions telles que les droits des animaux, l'environnement, l'antimondialisation, et la suprématie blanche. Le niveau de violence associé à ces thèmes nationaux a tendance à fluctuer, et tourne souvent autour d'événements ou de questions à l'ordre du jour. D'ailleurs, la grande majorité de ces activités relèvent bien du domaine de la protestation légitime. Ces

Contexte

LES ACTIVITÉS DU SCRS LIÉES AUX ENQUÊTES NATIONALES ET AUX QUESTIONS ÉMERGENTES

ÉTUDE DU CSARS



Ciblage
Lorsque le Service a des motifs raisonnables de soupçonner un individu ou une organisation de représenter une menace pour le Canada, il doit d'abord ouvrir une enquête. La figure ci-dessous indique le nombre de cibles (arrondi à la dizaine la plus proche) sur lesquelles le SCRS a enquêté au cours des trois derniers exercices financiers.

Des défis subsistent malgré les nouvelles directives et les changements organisationnels. Tout d'abord, la prévalence générale d'une attitude généralisée (au « sud ») d'indifférence envers le Nord du Canada. Celle-ci doit être surmontée à chaque fois que des considérations relatives aux enquêtes (ou à une demande subséquente de financement pour celles-ci) sont discutées. Ensuite, il existe des priorités opérationnelles au sud du pays (et à l'étranger) auxquelles on consacre la majeure partie des ressources du SCRS. Enfin, les restrictions budgétaires, toujours d'actualité, limitent les possibilités opérationnelles. À cela s'ajoute l'absence d'une stratégie du siège du SCRS visant à orienter les efforts du Service dans le Nord : le Service se repose sur les responsabilités régionales partagées, ce qui peut compliquer la priorisation des initiatives.

Le CSARS a constaté que, d'un commun d'accord, les gestionnaires du SCRS jugeaient le statu quo satisfaisant, mais que certains hauts fonctionnaires estimaient que sur le long terme (cinq ans ou plus), le siège du Service allait devoir jouer un rôle plus important. Le CSARS est de cet avis. Pour commencer, il serait bon que le SCRS mène une étude interne sur l'établissement d'une stratégie opérationnelle à long terme pour le Nord du Canada, comme il s'efforce de le faire avant une expansion à l'étranger. Une telle approche cadrerait bien avec l'importance de la question aux yeux du gouvernement, et permettrait de mieux positionner le Service pour faire face aux exigences de sécurité nationale quand elles prendront (et non « si elles prenaient ») de l'importance au sein de la frontière septentrionale du Canada.

Quelle que soit la manière spécifique dont une telle approche est mise en œuvre, le CSARS recommande que le SCRS « institutionnalise les responsabilités » en matière d'initiatives dans le Nord, et ce, en demandant au siège du Service d'établir des objectifs de liaison et opérationnels sur plusieurs années. Le Service doit aussi s'assurer que des ressources sont engagées à l'appui de tels objectifs.

Promouvoir les intérêts du gouvernement dans le Nord est devenue une priorité ces dernières années. Cette étude a porté sur la ou les raisons qui appuient les efforts du SCRS dans la sécurisation du périmètre nord du Canada. En particulier, l'étude a examiné l'ampleur de la ou des menaces telles qu'elles sont perçues par le Service, la façon dont les ressources consacrées à cette question sont gérées (au siège et dans les bureaux régionaux du SCRS), les activités de liaison du SCRS avec les partenaires du Nord et la façon dont les initiatives opérationnelles ont été élaborées et mises en œuvre.

En particulier, le CSARS a constaté que le SCRS faisait face à un certain nombre de défis imprévus suite à la décision du gouvernement en 2010 de désigner l'Arctique comme un « enjeu » en matière de renseignement et de sécurité. Le Service n'avait à ce jour pas joué de rôle important dans la collaboration avec les parties prenantes sur les enjeux liés au Nord. En l'absence d'un portefeuille dédié à l'Arctique, les ressources ont été utilisées pour enquêter sur ce qui avait été toujours été un nombre restreint de menaces. Le SCRS a donc dû faire face à une question qui, jusque-là, avait été considérée comme une priorité relativement faible.

Bien que le gouvernement ait encouragé le SCRS à réorienter ses ressources pour répondre à cette nouvelle priorité, le CSARS a constaté que les efforts du Service dans cette voie avaient été difficiles à mettre en œuvre en raison d'une autre priorité gouvernementale, les restrictions budgétaires. Celles-ci ont été décrétées précipitamment lorsque le SCRS tentait de réévaluer l'importance relative des menaces dans le Nord, leur complexité, et la façon dont les ressources devraient être consacrées au ciblage et au recrutement de sources. En 2011, le SCRS a reçu de nouvelles directives plus précises sur les attentes par rapport au Nord du Canada. Elles ont été suivies d'une réorganisation interne des responsabilités au sein du Service, visant à accroître l'efficacité et l'efficience des ressources dédiées au sujet. Le CSARS a constaté que suite à ces nouvelles directives et à la réorganisation régionale, la gestion stratégique du SCRS de la question du Nord était devenue plus cohérente avec l'approche adoptée pour d'autres responsabilités régionales.

À l'étranger ne sont plus l'exception, mais la norme actuelle. Des informations précises et à jour sur les agences étrangères sont donc cruciales, pour le succès de l'opération, mais aussi pour le maintien de bonnes relations de liaison.

Alors que les opérations à l'étranger prennent de l'importance et évoluent, l'exactitude des renseignements dans les profils d'ententes devient plus importante que jamais. Le CSARS recommande donc que le SCRS prenne des mesures immédiates pour s'assurer que les profils en vertu de l'article 17 sont toujours exacts, complets, à jour et pertinents.

ÉTUDE DU CSARS

L'APPUI DU SCRS AU PÉRIMÈTRE DE SÉCURITÉ DU NORD DU CANADA

Contexte

Le Nord du Canada est en plein bouleversement : il subit les impacts du changement climatique, bénéficie des progrès de l'exploitation minière et des hydrocarbures et de l'exploitation de ces ressources, ainsi que du développement des gouvernements et institutions autochtones et du Nord. Cependant, les regards qui se portent sur cette vaste région ne sont pas tous désintéressés : les questions de sécurité nationale dans le Nord, longtemps perçues comme une menace révolue après la guerre froide, reviennent sur le devant de la scène dans les médias, le domaine académique et au niveau du gouvernement.

Chacun des huit États circumpolaires (c.-à-d. le Canada, la Finlande, le Groenland [Danemark], l'Islande, la Norvège, la Russie, la Suède et les États-Unis) a sa propre définition de ce qui constitue la région circumpolaire, l'Arctique et le Nord. Le Canada tend à différencier le « Nord proche » du « Grand Nord ». Le Nord proche est généralement défini comme la masse terrestre entre 50° et 60° de latitude, tandis que le Grand Nord englobe toutes les régions situées au nord du 60° parallèle (c.-à-d. l'Arctique). Ces distinctions sont importantes pour le SCRS, car différentes considérations opérationnelles, financières et en matière de liaison, s'appliquent dans les activités dans le Nord proche et le Grand Nord du Canada.

existants, la réactivation des relations suspendues ou latentes, et la recherche de nouveaux partenariats. Dans certaines parties du monde, l'obligation de travailler et de traiter avec un petit nombre de partenaires qui peuvent poser problème est inévitable, et crée des défis supplémentaires. Cette réalité se juxtapose néanmoins à un questionnement raisonnable et à des recherches sur les antécédents douteux de certains de ces organismes et leur personnel.

Le Service peut, conformément à l'article 17 de la *Loi sur le SCRS*, conclure des ententes avec des entités étrangères. Un autre défi, tant en termes de travail de liaison que de conduite des opérations à l'étranger, est le risque de corruption dans certains de ces organismes. Dans une entente que le CSARS a examinée, des préoccupations antérieures relatives à la corruption avaient conduit à la suspension temporaire de cette relation. Ces possibles problèmes de corruption existaient toujours quand le Service a tenté de ranimer l'entente pour répondre à certains besoins opérationnels, mais il a adopté une approche progressive axée sur la gestion des risques. Le CSARS a constaté qu'avant de ranimer l'entente avec l'agence étrangère, le SCRS avait pris des mesures appropriées pour évaluer les problèmes actuels de corruption.

Les informations relatives aux ententes avec les entités étrangères se trouvent à l'article 17, « Ententes de coopération », de la *Loi sur le SCRS*. Ces profils d'ententes sont utilisés pour informer le directeur, les cadres, les directions et les bureaux régionaux, ainsi que les départements et entités externes, notamment le CSARS, leur précision et pertinence sont donc de la plus haute importance. Le Comité a constaté certaines lacunes en matière de contenu dans les trois profils d'ententes qu'il a examinés. Il a aussi noté que, dans au moins un cas, des informations essentielles contenues dans un dossier de source n'avaient pas été utilisées pour mettre le profil à jour.

Le CSARS avait déjà émis des commentaires sur l'exactitude et le maintien à jour des profils établis en vertu de l'article 17 et, malgré des progrès en ce qui concerne les mises à jour régulières, il reste un besoin d'améliorations significatif, notamment pour remplir les documents. Comme le CSARS a entendu tout au long de cette étude, les opérations

Étude du CSARS

Des éléments clés, notamment les critères d'ouverture et de fermeture des postes, les défis liés au travail à l'étranger, et l'évaluation des ententes avec des organismes étrangers, ont donné le ton de cette étude. Dans l'ensemble, le CSARS a constaté que le SCRS, qui essaie d'élargir son rôle opérationnel à l'étranger, adopte une approche stratégique et mise sur ses rôles en matière de liaison et d'activités opérationnelles. Néanmoins, le CSARS a souligné quelques problèmes notables, notamment l'exacuitude des renseignements fournis dans certains de ses profils d'ententes, la manière dont les priorités sont déterminées lors de la collecte de renseignements à l'étranger pour des besoins spécifiques, et les implications entourant la viabilité à long terme d'un rôle plus opérationnel plutôt qu'un rôle de liaison.

L'étude n'a pas pu répondre à la question générale de savoir si le SCRS était appelé à faire plus avec moins. Le CSARS a fait plutôt remarquer que la marque du SCRS à l'étranger évoluait au lieu de s'étendre, et que les exigences du gouvernement, notamment en matière de restrictions budgétaires, avaient encouragé une approche dynamique envers cette évolution. De nouvelles stratégies sont en place, et le SCRS espère qu'elles offriront la flexibilité nécessaire pour répondre à ses exigences en matière de collecte en cours et aux nouveaux enjeux qui pourraient surgir et demander l'attention du Service.

Cependant, pénétrer dans des zones riches en matière de collecte de renseignements présente des défis, et le CSARS a souligné que les possibilités existantes ne les résolvait pas complètement. Par exemple, le personnel d'un poste nous a décrit les défis de la gestion des exigences contradictoires auxquelles le SCRS doit faire face dans ses tâches administratives quotidiennes, ainsi que dans les fonctions de liaison clés et les activités opérationnelles complexes. Cet exemple souligne bien certaines des différences qui existent entre les postes qui se concentrent sur le travail de liaison et les postes plus opérationnels situés dans d'autres parties du monde.

L'évolution de la présence opérationnelle à l'étranger s'accompagne aussi avec des changements dans la façon dont le SCRS traite avec les agences de renseignement étrangères, notamment l'amélioration des dispositifs

ÉTUDE DU CSARS

L'ÉVOLUTION DE LA MARQUE DU SCRS À L'ÉTRANGER

Contexte

Les postes du SCRS à l'étranger sont situés à des endroits stratégiques afin de répondre aux besoins en matière de renseignement du gouvernement du Canada, et notamment l'appui au filtrage de sécurité des bureaux à l'étranger de Citoyenneté et Immigration Canada, la liaison avec d'autres partenaires (canadiens ou internationaux) situés à l'étranger, et la collecte de renseignements sur d'éventuelles menaces contre le Canada ou les intérêts canadiens. À l'exception des postes situés à Paris, Washington et Londres, et à la présence du SCRS en Afghanistan, l'emplacement des postes à l'étranger reste une information classifiée. D'habitude, les études du CSARS se penchent sur les efforts de liaison et les activités opérationnelles d'un seul poste à l'étranger. Cette année, le CSARS a adopté une perspective plus vaste, et a abordé la présence du SCRS à l'étranger au sens large du terme, en mettant l'accent sur le processus décisionnel autour de l'approche globale du Service en matière de représentation à l'étranger.

Service et en dehors de celui-ci.

Dans l'ensemble, le CSARS a constaté que le SCRS avait adopté une approche mesurée et prudente dans les initiatives examinées dans cette étude. La sécurité demeure de la plus haute importance et a été mentionnée à toutes les séances d'information du CSARS. Le Comité n'a vu aucun signe que des personnes soient incluses dans toute nouvelle initiative s'il était estimé que cela poserait un danger, ou si un certain succès n'était pas attendu. Le CSARS a également été rassuré de trouver un message cohérent soulignant le fait que l'objectif principal des bureaux régionaux et des programmes de collecte restait la collecte de renseignements au Canada, et que cette activité ne prendrait jamais le dessus sur la collecte de renseignements à l'étranger. En ce qui concerne les activités à l'étranger, le CSARS recommande que le SCRS élabore un cadre juridique décrivant les activités acceptables et interdites, notamment les niveaux d'approbation correspondants au sein même du Service et en dehors de celui-ci.

investissements importants effectués au Canada par des sociétés étrangères. Le rôle du SCRS dans le processus d'examen de la *Loi sur l'investissement Canada* est, en partie, de fournir des informations sur les investisseurs ainsi que leurs antécédents. Malgré les courts délais accordés à ce travail, le Service est un maillon important du processus global dans lequel le ministre de la Sécurité publique aide le ministre de l'Industrie à déterminer si l'investissement proposé pourrait être ou serait préjudiciable.

Les récents accords du Canada en matière de politique étrangère et de commerce international se traduiront probablement par de plus grandes exigences des clients pour obtenir des informations sur les sociétés d'État étrangères, et autres questions ayant trait à l'économie ou à la prospérité du pays. Le CSARS suivra l'évolution de la participation du SCRS dans ces processus avec intérêt dans les années à venir.

Dans ce dossier, le CSARS a conclu que le SCRS avait globalement agi de façon appropriée en vertu des politiques opérationnelles actuelles. Cependant, quelques ajustements pourraient être nécessaires au fur et à mesure que les nations étrangères élaboreront de nouvelles stratégies. Il sera intéressant pour le CSARS de voir quelle tournure prendront les enquêtes du SCRS sur les menaces posées par l'espionnage et les activités influencées par l'étranger des gouvernements étrangers.

ÉTUDE DU CSARS

LES INITIATIVES DU SCRS EN MATIÈRE DE COLLECTE À L'ÉTRANGER

Contexte

En février 2013, le directeur du SCRS, Richard Fadden, notait que le Service savait que « des dizaines de Canadiens » ont voyagé à l'étranger ou ont tenté de le faire pour se livrer à des activités liées au terrorisme. Le SCRS espère que les activités de collecte à l'étranger aideront à combler ce manque d'information. En effet, le CSARS a aussi vu comment l'orientation du gouvernement et les questions émergentes, comme les enlèvements et les migrations illégales, demandaient au Service de faire état des activités à l'étranger. Les opérations de collecte à l'étranger permettent au SCRS d'identifier les menaces avant qu'elles ne touchent le

Canada, et l'aident à moins dépendre des rapports des alliés, en concentrant ses efforts de collecte sur les menaces d'origine étrangère pour le pays.

Étude du CSARS

Cette étude s'est penchée sur les efforts de deux directions pour améliorer leurs capacités de collecte de renseignements à l'étranger. Elle prolonge l'examen en cours du CSARS sur la façon dont le SCRS fonctionne à l'étranger avec les services de renseignement partenaires, tout en travaillant de façon autonome pour combler les lacunes en matière de renseignement. Les deux directions ont travaillé avec les différents bureaux régionaux du SCRS afin d'élaborer des cadres définissant les priorités en matière de collecte de renseignements, les méthodes et les buts de la collecte à l'étranger, et les liens de celles-ci aux préoccupations canadiennes. Les documents décrivant ces initiatives sont fréquemment mis à jour pour refléter l'évolution constante de la menace ou les changements sur les lacunes en matière de renseignement.

En mars 2012, le SCRS a créé une unité dédiée à la formation sur les opérations, et ce, en partie parce que le Service a reconnu qu'il s'aventurait davantage dans des zones plus dangereuses. Les modules de formation sont adaptés à l'opération en question, et comprennent un mécanisme de réaction. L'intégration systématique d'un tel mécanisme est un excellent moyen d'assurer une meilleure formation, et le CSARS a constaté que les leçons apprises et l'approche itérative adoptée dans l'élaboration des modules de formation étaient une bonne pratique.

L'un des avantages majeurs de ces modules de formation est de permettre au SCRS de poser un regard critique sur les lacunes opérationnelles, et ce, façon continue. La formation et l'évaluation peuvent également introduire une certaine dose d'objectivité, et aider à atténuer les divergences d'opinions quand il s'agit de décider d'opérer dans un milieu potentiellement dangereux. Le CSARS soutient le développement de la formation opérationnelle, et recommande que le Service veille à ce que toutes les personnes jugées prioritaires pour la formation en bénéficient, surtout si elles travaillent dans un milieu dangereux.

relèvent du cadre diplomatique, ces activités sont considérées comme une menace et dignes de l'intérêt du SCRS quand ces personnes essaient secrètement d'obtenir des informations ou d'influencer la prise de décision.

L'un des défis du SCRS est de continuer à faire la distinction entre les activités dites clandestines et celles qui relèvent de la diplomatie légitime. Autrefois, déceler des formes dissimulées d'influence étrangère était peut-être plus simple, car des approches traditionnelles étaient utilisées et les agents d'influence étrangers faisaient généralement l'objet d'enquêtes du Service. Cependant, les méthodes auxquelles les acteurs étrangers ont recours évoluent constamment.

Dans le cas des activités influencées par l'étranger examinées ici, les aspects négatifs se posent clairement : les principes démocratiques sont remis en question par un gouvernement étranger. Toutefois, les éléments clandestins de ces activités ne sont pas si évidents. Du point de vue du Comité, un certain nombre d'activités qui donnent lieu à une enquête semblent être menées au grand jour, et non de façon clandestine. Le CSARS a noté que, bien que les activités des États étrangers pouvaient être organisées et ciblées, leur caractère ne constituait pas en lui-même un indicateur d'activité secrète.

Les enquêtes sur l'espionnage et les activités influencées par l'étranger continuent de prendre de l'ampleur et de gagner en complexité, et le défi de faire la distinction entre ce qui est clandestin et ce qui est légitime sera aussi de taille. Le CSARS estime que clarifier cette distinction est important, car la collecte d'informations sur les questions liées à la menace doit, conformément à la *Loi sur le SCRS*, être « strictement nécessaire ». Le CSARS recommande que le SCRS réajuste de façon appropriée ses politiques et pratiques, et ce, pour aider les enquêteurs et analystes à identifier des seuils communs et cohérents, et pour évaluer quand une activité passe dans le domaine clandestin.

Peaufiner l'approche

Au cours des dernières années, les agents d'ingérence étrangers ont ciblé des personnes et des groupes dans de plus petites tranches de la société canadienne, et ce, afin de tirer parti de ces relations pour gagner une plus grande influence au niveau national. Par exemple, certains éléments étrangers ont tenté de

se rapprocher de diverses tranches de la société pour possiblement tenter de contourner d'autres autorités, comme le gouvernement fédéral, ou les gouvernements provinciaux ou municipaux. Souvent, le SCRS alerte les parties concernées (par exemple, des hommes politiques, des dirigeants d'entreprises, des universitaires et autres personnalités influentes) en leur offrant des informations et des conseils en matière de sécurité, mais toutes les communautés touchées ne bénéficiaient pas de telles mesures.

Le SCRS préfère parfois l'approche attentiste pour plusieurs raisons. Il se peut que le Service n'ait pas suffisamment d'informations précises sur les cibles potentielles ou sur la stratégie offensive prévue. Il est également préoccupé par la façon dont son message, quel qu'il soit, peut être perçu par certaines communautés, et si ce message sera vu de manière positive. Le Comité reconnaît les préoccupations du Service, néanmoins, ne pas informer toutes les communautés canadiennes des questions de sécurité autour d'une menace particulière, mais renseigner les autres pans de la société, pose problème. En essayant de rassembler des informations sur les activités influencées par l'étranger sans en informer toutes les communautés, le SCRS pourrait causer davantage de méfiance, surtout si ces communautés apprennent les activités du Service par d'autres moyens. Ainsi, le CSARS recommande que le SCRS élabore une stratégie visant à offrir les mêmes messages d'avertissement sur les activités influencées par l'étranger à tous les secteurs potentiellement touchés par de telles activités.

Une inquiétude croissante

Au cours des dernières années, le gouvernement du Canada a montré un intérêt croissant envers les risques potentiels pour la sécurité nationale posés par les sociétés d'État étrangères. Le SCRS a informé le CSARS que les conseils que le Service prodigue au gouvernement du Canada sur ces sociétés ne visaient pas à mettre un terme aux investissements, mais plutôt à informer le gouvernement pour qu'il prenne des décisions éclairées en matière de commerce et de relations avec les partenaires étrangers. Le SCRS participe également au processus de la *Loi sur l'investissement Canada*. Le Règlement sur les investissements susceptibles de porter atteinte à la sécurité nationale a été enregistré en 2009, et il est devenu un nouveau secteur d'activité pour le SCRS. L'un des buts de la *Loi sur l'investissement Canada* est d'examiner les

charge le dossier sur la base d'une entente informelle régissant les interactions entre la communauté du Groupe des cinq. Néanmoins, il est entendu que chaque nation alliée se réserve le droit d'agir dans son propre intérêt national. Par exemple, la législation sur la sécurité nationale aux États-Unis et au Royaume-Uni leur donne le pouvoir de se réserver l'information et d'agir en conséquence si elle touche à la sécurité nationale, et ce, même si elle a été recueillie pour le compte d'un autre pays, comme le Canada.

Le risque auquel le SCRS fait donc face est la capacité d'un partenaire de la communauté du Groupe des cinq d'agir indépendamment sur la base des informations provenant du Service. Cela pourrait conduire à la détention d'une cible, ou à un préjudice envers celle-ci, et ce, toujours sur la base d'informations provenant du Service. Le CSARS a conclu que même si miser sur des partenaires dans le cadre de l'exécution de ce nouveau pouvoir octroyé au moyen de mandat présentait des avantages (et le recours à la communauté est essentiel pour que le processus soit efficace), des risques clairs se posaient également, notamment le manque de contrôle sur l'information une fois partagée.

Conclusions

Le CSARS a noté des signes que le Service avait commencé à utiliser des mises en garde qui stipulent que les organismes alliés doivent communiquer avec le SCRS s'ils agissent sur la base d'informations provenant du Service. Les mises en garde, sous leur forme actuelle, sont toujours considérées comme un « travail en cours » par le Service, mais elles ne répondent pas encore à la réalité plus vaste de ce type de collecte de renseignements. Néanmoins, elles restent un outil utile et, dans une certaine mesure, offrent au Service une protection, qui comporte cependant des défis, notamment le contrôle de l'information qu'il cherche à recueillir. Le CSARS a recommandé au SCRS de concevoir un système de protection approprié pour le partage de l'information émanant du Service, et de se tenir informé du mieux possible sur l'usage potentiel de ses informations.

En outre, la plupart de ces mises en garde, qui rentrent dans le cadre plus large du régime des « garanties », n'ont été utilisées qu'avec un partenaire. Le CSARS recommande donc que, dans le cadre de ce nouveau pouvoir octroyé au moyen de mandat, le SCRS

étende l'usage de mises en garde et de garanties aux organismes de toute la communauté du Groupe des cinq, afin de s'assurer que nulle information ne soit diffusée à l'insu du Service.

ÉTUDE DU CSARS

LE TRAVAIL D'ENQUÊTE LIÉ À L'ESPIONNAGE ET À L'INFLUENCE ÉTRANGÈRE

Contexte

La priorité numéro un pour le SCRS reste la lutte contre les menaces terroristes. Cependant, le Canada fait face à un niveau d'activité d'espionnage comparable à celui qui existait lors de la guerre froide, et les nations impliquées dans ces activités parrainées par l'État changent de tactique. Afin de répondre à ce défi, le rôle principal du SCRS est de conseiller les ministères du gouvernement du Canada pour les aider à mieux comprendre les menaces émergentes liées aux nouvelles formes d'espionnage et de contre-espionnage, et à demeurer conscients des intérêts de certaines nations en matière de politique étrangère, de commerce et de renseignements.

Étude du CSARS

Cette étude a examiné la manière dont le SCRS fait face à la menace posée par l'évolution rapide des activités d'espionnage et d'influence de nations étrangères. Du point de vue du Service, les nouveaux défis et la complexité des enquêtes sur ces activités sont autant d'occasions de regarder au-delà des formes traditionnelles d'espionnage et de se plonger dans de nouveaux domaines opérationnels. Le CSARS s'est ici penché sur les conseils que le SCRS prodigue face à différentes formes d'activités influencées par l'étranger. Au sein même du pays, diplomates, officiers du renseignement, et dirigeants d'entreprises nationales étrangères mènent des activités clandestines afin de faire progresser les intérêts de leurs pays respectifs – ces pratiques existent depuis longtemps. De telles activités influencées par l'étranger deviennent plus graves lorsque les cibles stratégiques sont de hauts fonctionnaires canadiens ou d'éminents membres des milieux d'affaires. Bien que certaines des relations stratégiques que mènent les représentants nationaux étrangers

MANDATS			
Nouveaux mandats			
	2010-11	2011-12	2012-13
Mandats remplacés ou mandats supplémentaires	176	156	165
Total	231	206	236

Étude du CSARS

Au cours de la période durant laquelle l'étude a été menée, 35 mandats (plus sept mandats supplémentaires) ont été décernés par voie du nouveau pouvoir. Le Comité a constaté que plusieurs défis s'étaient posés au SCRS, notamment l'efficacité de la collecte de renseignements, le contrôle sur l'information recueillie, et des attentes peut-être irréalistes pour l'avenir. En effet, il a été noté que s'appuyer sur des organismes partenaires canadiens et étrangers pour la collecte de renseignements se fait finalement au détriment d'une certaine efficacité. De grands progrès ont été faits depuis l'émission du premier mandat, mais le SCRS est encore dans une phase d'apprentissage et le Service devra gérer les attentes et les réalités, notamment les limites, des rapports s'appuyant sur des renseignements ainsi obtenus.

Dans presque tous les cas, le SCRS mise sur la communauté du Groupe des cinq (soit le Canada, les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande) pour tirer le meilleur parti de la collecte de renseignements dans le cadre du nouveau pouvoir octroyé au moyen de mandat. Le CSARS a noté que, même avec l'aide d'alliés, la collecte de renseignements ou les informations obtenues par voie de ce pouvoir avaient présenté des avantages et des défis que le Service n'avait initialement pas prévu.

Les ententes avec les partenaires et alliés donnent aussi à d'autres organismes la possibilité d'agir indépendamment sur la base des informations provenant du SCRS. Dans la pratique, si un organisme allié collecte des renseignements sur un citoyen canadien, c'est un organisme canadien qui devrait idéalement prendre en

cette Stratégie, l'étude du Comité a constaté qu'il y avait encore du travail à faire pour coordonner les activités liées à l'Internet du SCRS avec celles du CSTC, en particulier en ce qui concerne la protection d'information et d'infrastructures électroniques d'importance du gouvernement du Canada.

Compte tenu de l'inévitable de la coopération accrue entre le CSTC et le SCRS, le CSARS recommande que le SCRS élabore des principes généraux de coopération entre les deux organisations plus clairs et plus solides. Ces principes devraient répondre au nombre croissant de défis qui ont surgi entre les deux entités, tout en respectant leurs mandats respectifs.

ÉTUDE DU CSARS

EXAMEN DU NOUVEAU POUVOIR OCTROYÉ AU MOYEN DE MANDAT EN VERTU DE L'ARTICLE 21

Contexte

Il s'agit là du premier examen du CSARS d'un nouveau pouvoir octroyé au moyen de mandat en vertu de l'article 21 de la *Loi sur le SCRS*, qui a été à l'origine autorisé par la Cour fédérale en 2009. Il lui a été octroyé pour que le Service puisse continuer à suivre les cibles qui représentent une menace pour le Canada lorsqu'elles voyagent à l'étranger ou, dans certains cas, y résident. L'étude s'est penchée sur les processus, les politiques et les contrôles que le SCRS a mis en place pour gérer ce nouveau pouvoir, ainsi que sur la coopération et les échanges avec des partenaires canadiens du Service. Elle a également cherché à évaluer l'importance de l'information, obtenue par voie de ce pouvoir, pour les enquêtes du Service.

de la Nouvelle-Zélande. Dans son rapport annuel 2011-2012, le Bureau du commissaire du CSTC notait que « compte tenu de la complexité croissante des défis technologiques, cette alliance axée sur la coopération peut être plus précieuse que jamais auparavant ».

De son côté, le SCRS estime que les échanges avec le CSTC ne présentent que de faibles risques. En effet, en dehors du partage, au sens large du terme, des informations, les agences alliées de SIGINT se concentrent principalement sur leurs propres priorités nationales en matière de renseignement. Toutefois, le CSARS est plus préoccupé par les cas dans lesquels les priorités de collecte de renseignements des alliées se sont heurtées à celles du Canada, comme dans les affaires de contre-terrorisme.

Le SCRS reçoit une orientation du ministre et a ses propres politiques pour prévenir l'utilisation abusive des renseignements et leur mauvaise utilisation, tant sur le plan de la sécurité que dans la perspective des droits de la personne. Cependant, le Comité ne voit pas très bien comment le SCRS peut se conformer aux instructions ministérielles stipulant que les mises en garde doivent être utilisées lors du partage de l'information avec des destinataires nationaux et étrangers alors que la nature même de collecte et de diffusion de SIGINT va à l'encontre de ce principe.

Le Service a avoué au CSARS que répondre à ces préoccupations était loin d'être simple, et que cela demeurerait un « travail en cours ». Avec la collaboration plus poussée entre le SCRS et le CSTC, le Comité d'évaluer les progrès qui ont été accomplis pour relever ce défi.

Un dernier enjeu : la cybersécurité

Dans la dernière section de cette étude, nous avons relevé une anomalie dans la relation entre le SCRS et le CSTC : un manque avéré de coopération en matière de cybersécurité. En 2010, Sécurité publique Canada a mis sur pied une stratégie pangouvernementale, la Stratégie de cybersécurité du Canada (la Stratégie), qui stipule qu'il ne peut y avoir aucune ambiguïté dans le rôle de chacun. La Stratégie confirme les rôles respectifs du CSTC et du SCRS : le premier est un expert reconnu dans le traitement des cybermenaces et des attaques, et ce dernier est, généralement parlant, chargé d'analyser les menaces nationales et internationales et d'enquêter sur celles-ci. Malgré

De son côté, le SCRS a reconnu les difficultés liées au chevauchement des mandats et, bien souvent, le problème des exigences particulières de l'implémentation des activités liées au déploiement ou à l'utilisation des sources humaines du SCRS ou de la technologie du CSTC. Parmi les solutions à ces problèmes présentées au Service, on note : mieux former les bureaux opérationnels du CSTC et du SCRS aux politiques pertinentes, et mettre sur pied un conseil d'administration des opérations pour assurer la gestion stratégique de ces activités.

Partage de l'information

En dépit de l'encart qui précède, une grande partie de l'étude s'est penchée sur la façon dont le CSTC et le SCRS partagent les informations. Normalement, à chaque fois que le SCRS partage des informations, il utilise des « mises en garde » et/ou des « assurances ». Une mise en garde précise que l'information fournie appartient au SCRS, et ne peut être transmise à un autre organisme ou modifiée sans le consentement direct du Service. Une assurance est un accord bilatéral formel pris avec des organismes étrangers, et qui stipule que les informations du SCRS ne seront pas utilisées d'une manière qui va à l'encontre des conventions internationales relatives aux droits de la personne. La mesure dans laquelle les mises en garde et/ou les assurances sont efficaces dépend du degré de confiance entre le SCRS et l'organisation qui bénéficie des informations. Le CSARS a cependant constaté que davantage de collaboration entre le renseignement humain et le renseignement d'origine électromagnétique pouvait conduire à la perte potentielle de contrôle sur l'information partagée.

Si le Comité est parvenu à cette conclusion, c'est que les mises en garde et les assurances du SCRS n'ont jamais été conçues pour la collecte de renseignement d'origine électromagnétique. Contrairement à la collecte de renseignement humain, qui se fait souvent de façon autonome (à savoir recueillir des informations auprès d'une source humaine et, si on le désire, partager ensuite ces informations avec une organisation alliée), la collecte de renseignement d'origine électromagnétique est davantage un travail de groupe. Le CSTC appartient à une alliance spéciale qui comprend la National Security Agency (États-Unis), le Service gouvernemental d'écoutes et de transmissions (Royaume-Uni), le Defence Signals Directorate (Australie) et le Bureau de la sécurité des communications du gouvernement

ÉTUDE DU CSARS

LES RELATIONS ET ÉCHANGES DU SCRS
AVEC LE CENTRE DE LA SÉCURITÉ DES
TÉLÉCOMMUNICATIONS CANADA (CSTC)

Contexte

La décision du gouvernement d'installer le siège du CSTC à côté du siège du SCRS illustre bien la tendance générale de fusionnement accru des mondes du renseignement d'origine humaine (HUMINT) et du renseignement d'origine électromagnétique (SIGINT), mondes autrefois bien distincts. Cette tendance s'est nourrie d'exigences gouvernementales de plus en plus grandes pour obtenir des renseignements pertinents de façon rapide, et ce, afin de maximiser l'efficacité opérationnelle dans un contexte de restrictions budgétaires, et de faire face à un contexte mondial de la menace en pleine évolution et de plus en plus complexe du point de vue technologique.

Cette étude, qui a examiné les initiatives opérationnelles et non opérationnelles, traite des avantages, pour le Service, d'une coopération accrue avec le CSTC. Elle s'est penchée sur les efforts concertés pour coordonner les services partagés, pour assurer un transfert inter-organisationnel des connaissances suffisant, la façon dont les risques opérationnels sont gérés, la collecte de renseignements sans rapport avec la menace (cf. l'article 16 de la *Loi sur le SCRS*), et la pertinence de l'orientation et des politiques utilisées pour guider le SCRS dans son partage des renseignements avec le CSTC.

LA COLLECTE DE RENSEIGNEMENTS ÉTRANGERS

L'article 16 de la *Loi sur le SCRS* définit le renseignement étranger comme toute information sur les moyens, les intentions ou les activités d'un État étranger, d'une organisation nationale ou d'un ressortissant étranger (c.-à-d. des renseignements sans rapport avec la menace). En revanche, l'article 12 de la *Loi* définit le renseignement de sécurité comme des informations et renseignements liés aux « menaces envers la sécurité du Canada ». Malgré la grande coopération avec le CSTC dans les activités de collecte de renseignements étrangers au Canada, le Service continue de débattre à l'interne sur la mesure dans laquelle ces activités ont un impact négatif sur le mandat principal du SCRS, qui est de recueillir des renseignements de sécurité. Après avoir écouté diverses sources du SCRS sur cette question, le Comité a mis en garde le Service, l'incitant à la prudence pour décider dans quelle mesure il continue à demander l'aide du CSTC dans le cadre de l'article 16. À moins que des modifications soient apportées à la *Loi sur le SCRS*, c'est le CSTC, et non le SCRS, qui est l'organisation principalement chargée de fournir au gouvernement du Canada des renseignements étrangers.

Étude du CSARS

L'étude a révélé qu'un certain nombre de défis empêchaient le SCRS et le CSTC de tirer pleinement parti des possibilités offertes par la nouvelle proximité de leurs sièges respectifs. Pour des organismes de renseignement en proie avec un problème accru de restriction de ressources, le partage de services permet une gestion efficace de celles-ci. Malheureusement, le Comité a constaté que les attentes initiales à ce sujet avaient peut-être été un peu trop grandes. Bien que le CSTC n'ait pas encore pris pleinement possession des lieux, et que donc les bénéfices puissent être meilleurs que prévu, dans une large mesure, les avantages potentiels ont jusqu'à présent été minés par des problèmes de gestion, les restrictions budgétaires et des complications liées à l'installation du CSTC. Globalement, le CSARS a constaté que le SCRS et le CSTC avaient des difficultés à comprendre leurs mandats respectifs et leurs responsabilités respectives. Cette entrave à la coopération a été soulevée aux niveaux opérationnel et de la gestion dans les directions opérationnelles du SCRS, et le problème a été reconnu lors des réunions conjointes des deux organisations. En outre, à cause de ces lacunes, dans certains cas, les politiques ou les procédures du SCRS n'ont pas été respectées, ce qui aurait pu avoir un impact négatif sur les risques liés aux opérations.

Le CSARS note avec satisfaction que le SCRS a donné suite à plusieurs de ces recommandations. Ainsi, le SCRS a été d'accord avec la recommandation faite par le Comité dans le rapport annuel 2011-2012 de mettre à jour la politique du Service sur les mises en garde, et ce, de manière à refléter les pratiques et processus actuels d'échange d'information avec les partenaires étrangers.

de questions.

Ce processus fournit aussi au SCRS l'occasion de répondre officiellement aux études et aux décisions du CSARS et il s'inscrit dans le dialogue constant entre les deux organismes. Au cours de la période d'étude de 2011-2012, le CSARS a formulé neuf recommandations portant sur un vaste éventail de questions.

Chaque année, le CSARS demande au SCRS un rapport indiquant où il en est par rapport aux recommandations formulées dans les études et les décisions prises à l'égard de plaintes pendant l'exercice précédent. Ce rapport lui permet d'assurer un suivi de la mise en œuvre de ses recommandations et d'en vérifier les effets concrets sur le SCRS.

SUIVI DES RECOMMANDATIONS DU CSARS

Les chercheurs du CSARS consultent de nombreuses sources d'information lorsqu'ils se penchent sur des aspects particuliers des travaux du Service. Dans le cadre de ce processus, ils peuvent organiser des séances d'information avec des employés du SCRS et étudier les dossiers d'enquête sur des individus et des groupes, les dossiers de sources humaines, les évaluations de renseignements et les documents joints aux demandes de mandats.

Le CSARS peut aussi examiner les dossiers ayant trait à la coopération et aux échanges opérationnels du SCRS avec des services et des partenaires étrangers et canadiens, entre autres sources, qui peuvent différer d'une étude à l'autre. L'idée de cette multiplicité de sources est que le CSARS puisse scruter un corpus

Chaque étude fournit un instantané des actions présentes au ministre de la Sécurité publique.

Le rapport annuel classifié que le directeur du SCRS par le SCRS ou le touchant;

Les nouvelles orientations et initiatives annoncées de sa fonction relative aux plaintes;

Les questions cernées par le CSARS dans le cadre d'activités du SCRS qui pourraient avoir une incidence sur les droits et libertés individuels;

Le rapport annuel classifié que le directeur du SCRS présente au ministre de la Sécurité publique.

L'IMPORTANCE DE LA REDDITION DE COMPTES

Les études du Comité contiennent des constatations et, s'il y a lieu, des recommandations. Elles sont remises au directeur du SCRS et à Sécurité publique Canada.

Le CSARS est l'un des divers mécanismes qui visent à assurer la reddition de comptes au sujet du SCRS. Celui-ci doit aussi rendre compte de ses opérations par l'entremise du ministre de la Sécurité publique, des tribunaux, des organismes centraux du gouvernement (p. ex. le Bureau du Conseil privé et le Secrétaire du Conseil du Trésor), du vérificateur général du Canada ainsi que des commissaires à l'information et à la protection de la vie privée du Canada.

d'informations assez varié pour avoir la certitude d'examiner et de comprendre à fond les dossiers en cause.

POUR EN SAVOIR PLUS À PROPOS DES ÉTUDES ANTÉRIEURES DU CSARS

Au fil des ans, le CSARS a étudié un vaste éventail d'activités du SCRS. La liste complète des études antérieures du Comité figure sur son site Web (www.sirc-csars.gc.ca)

SECTION 2

RÉSUMÉS DES ÉTUDES DU CSARS ET DES PLAINTES

A. ÉTUDES

Les études du CSARS visent à fournir au Parlement et à la population canadienne un tableau complet des activités du Service sur le plan opérationnel. Lorsqu'il effectue ses études, le CSARS examine la manière dont le SCRS s'est acquitté de ses fonctions afin de déterminer, après le fait, si celui-ci a agi d'une manière appropriée et efficace et conforme à la loi.

QUELLE DIFFÉRENCE Y A-T-IL ENTRE UN ORGANISME DE CONTRÔLE ET UN ORGANISME DE SURVEILLANCE?

Un organisme de contrôle examine en permanence ce qui se passe au sein d'un service de renseignement et il a pour mandat d'en valuer et d'en contrôler les activités. Le CSARS est un organisme de surveillance de sorte que, contrairement à un organisme de contrôle, il peut évaluer périodiquement le rendement du SCRS sans avoir eu part à ses décisions opérationnelles et à ses activités de quelque manière que ce soit.

MANIÈRE DE CONDUIRE LES ÉTUDES

Les études du CSARS fournissent un examen rétrospectif et une évaluation des enquêtes et activités particulières du SCRS. Son programme de recherches est conçu de manière à englober un vaste éventail de sujets, et à le faire en temps utile et par thème.

- Lorsqu'il détermine les sujets qu'il compte examiner, le CSARS prend en considération :
- ▶ les événements ou les faits nouveaux susceptibles de menacer la sécurité du Canada;
 - ▶ les priorités établies par le gouvernement du Canada en matière de renseignement;

Il est intéressant de noter un contraste entre les grands thèmes identifiés dans le reste des études du CSARS discutées ci-dessus. L'examen de l'affaire Abdelrazik porte sur les activités du SCRS dans la première moitié des années 2000, une époque où tout restait encore à faire dans le cadre des lignes directrices et des décisions en matière d'opérations à l'étranger. Comme le CSARS a souligné dans son étude, il n'est pas surprenant que le Comité n'ait pas fait, ici, de nouvelles recommandations, car les changements de politique du SCRS et les recommandations antérieures du Comité avaient déjà répondu aux préoccupations que le cas avait soulevées. Au début et au milieu des années 2000, le SCRS, le gouvernement et la population canadienne se demandaient encore si les activités du SCRS devaient s'étendre à l'étranger, dans quelle mesure, et les répercussions qu'un tel développement aurait sur le Service et toute la communauté canadienne du renseignement.

En 2013, le débat est passé à l'étape suivante. La discussion porte désormais sur la façon dont le travail pourrait être mieux fait, les lacunes qui subsistent dans les politiques et procédures du SCRS pour opérer dans le contexte actuel du renseignement de sécurité, et les mesures en place et appliquées pour assurer l'exercice continu des pouvoirs du Service dans les limites de son mandat.

Cette année, cinq plaintes ont été réglées. Comme dans les études du CSARS, les recommandations émises dans ces affaires visent à combler des lacunes et à assurer une meilleure normalisation des pratiques

RÉSoudre DES PLAINTES

Le dernier exemple d'étude de l'institutionnalisation des responsabilités a émergé de la remise du certificat du CSARS au rapport annuel du directeur du SCRS présenté au ministre de la Sécurité publique. Dans l'ensemble, le CSARS a été satisfait de la qualité et l'exhaustivité du rapport du directeur. Cependant, le Comité a constaté que le volume et le détail des informations incluses dans le rapport décrivant les opérations du SCRS à l'étranger n'étaient pas aussi exhaustifs qu'ils auraient pu l'être. Étant donné que cette section vise à fournir au ministre une solide compréhension des menaces de plus en plus grandes auxquelles les employés du Service font face lors des opérations à l'étranger, le CSARS estime que des renseignements plus détaillés fourniraient une description plus précise et plus représentative des activités du SCRS. Le CSARS a noté que le directeur du SCRS pourrait fournir plus d'informations dans ce domaine l'année prochaine, et que la question est suffisamment importante pour qu'on y prête une attention continue et que le ministre s'y intéresse.

mouvements écologistes extrémistes, les mouvements de suprématie blanche, et l'extrémisme sécessionniste, ont, à des degrés divers, été perdues de vue. Par conséquent, le SCRS a réévalué et remanié ces enquêtes pour laisser de côté les zones qui montraient peu de signes de menace active, tout en recatégorisant les idéologies extrémistes (gauche, droite, etc.) pour se concentrer sur le potentiel de violence plutôt que sur l'orientation idéologique. Ceci a abouti à la fin du suivi et des enquêtes sur certaines cibles de longue date de moins en moins actives. Le risque résiduel demeure la possibilité d'une soudaine flambée de violence au Canada, provoquant une demande immédiate de renseignements du gouvernement. Pour atténuer ce risque, le CSARS a noté et encouragé la stratégie du SCRS qui est de maintenir une liaison active avec ses partenaires canadiens, notamment ceux du maintien de l'ordre, qui suivent ces mêmes groupes en raison de leurs activités criminelles.

Cependant, dix ans se sont écoulés depuis la plupart des événements décrits dans le rapport, et les mesures correctives et les recommandations répondant de façon satisfaisante aux préoccupations du Comité ont déjà été couvertes dans ses rapports antérieurs, ainsi que par des commissions d'enquête. Le CSARS encourage les SCRS à profiter de cette étude pour revoir toutes les recommandations du Comité faites ces dix dernières années; toutefois, nous n'avons pas proposé de nouvelles recommandations, qui auraient été redondantes.

Cette année, le CSARS a terminé l'examen du rôle du SCRS dans l'affaire Abdelrazik. Dans son étude, le CSARS a conclu qu'il n'y avait aucune indication que le SCRS avait demandé aux autorités soudanaises d'arrêter ou de détenir M. Abdelrazik, mais le Comité a constaté que le SCRS avait tenu ses alliés informés des derniers renseignements concernant son cas une fois qu'il était parti du Canada. De plus, le CSARS a constaté que les deux organisations gouvernementales canadiennes les plus fortement impliquées dans cette affaire avaient mené leurs tâches consulaires et leur travail en matière de renseignement en même temps, parfois en se contredisant. Le CSARS a aussi fait part d'inquiétudes sur la divulgation inappropriée d'informations classifiées, la production d'une évaluation exagérée de certains renseignements, transmis de façon inexacte aux partenaires du gouvernement du Canada, et l'établissement de trop nombreux rapports dans les bases d'informations de renseignements opérationnels non liés à la menace, et provenant de personnes qui n'étaient pas des cibles.

ABDELRAZIK BOUCLER LA BOUCLE : L'AFFAIRE

du Service. Par exemple, dans le cas d'une plainte au sujet du processus d'entrevue aux fins d'immigration, le CSARS a recommandé que le SCRS adopte la pratique d'une région, qui de tousjours préparer et tester les appareils d'enregistrement avant l'entrevue, et que cette pratique soit appliquée à tous les bureaux régionaux du Service. Dans une autre affaire, le CSARS a noté qu'il fallait périodiquement revoir les cas dans lesquels les employés du gouvernement pouvaient divulguer le nom de leur employeur, et les conditions dans lesquelles ils pouvaient le faire.

étrangères dans le domaine de la cybermétrique. Le Comité a constaté que l'un des défis majeurs de la collecte et de l'analyse d'informations sur l'espionnage est, comme cela a souvent été, de faire le tri entre les activités « légitimes » d'un État menées au sein du pays et toutes les activités « clandestines ».

Compte tenu de la gamme interminable de plates-formes au sein desquelles les activités d'espionnage peuvent maintenant être menées et de techniques auxquelles on peut avoir recours, le SCRS doit relever un défi de taille : rester dans les limites « strictement nécessaires » des pouvoirs qui lui sont accordés en vertu de la *Loi sur le SCRS*. Par conséquent, le CSARS a recommandé que le SCRS peaufine ses politiques et pratiques existantes dans ce domaine, et ce, pour aider les enquêteurs à identifier des limites communes et cohérentes, et à élaborer des indicateurs et outils plus solides pour définir les activités qui relèvent du domaine clandestin.

Une autre étude du CSARS s'est penchée sur certaines des initiatives en cours pour soutenir les programmes de collecte de renseignements du SCRS à l'étranger. Le Service avait établi la nécessité et le mandat d'une telle collecte, et est maintenant passé à la phase d'évaluation et d'amélioration des outils et des politiques qui mettent en évidence ce rôle et établissent sa capacité à le mener. Le CSARS s'est montré satisfait de ce qu'il a estimé être un message cohérent dans toutes les directions du Service; message qui maintient que les activités de collecte de renseignements à l'étranger ont toujours un lien solide avec le Canada, et qu'on ne les laisse jamais prendre priorité sur les enquêtes menées au pays. Toutefois, avec la multiplication des défs opérationnels et juridiques pour mener de telles activités en dehors du Canada, le CSARS a identifié des lacunes sur lesquelles le SCRS doit se pencher, tant en matière d'accès à la formation (en particulier pour les personnes déployées dans des milieux dangereux) qu'en matière de limites légales des activités de collecte de renseignements. Les opérations du SCRS à l'étranger redessinent la donne, et, devant les opportunités et les risques potentiels qu'elles représentent, le SCRS va devoir élaborer un cadre juridique plus complet pour définir clairement les types d'activités acceptables et interdites.

Dans une autre étude du CSARS, l'examen annuel des postes à l'étranger, nous avons estimé que les opérations du SCRS à l'étranger ne prenaient pas tant d'ampleur, mais plutôt qu'elles évoluaient. Dans le contexte fiscal actuel de contraintes financières, le SCRS ne peut pas consacrer la même énergie à chaque source opérationnelle potentielle étrangère (et elles sont nombreuses) dont il est au courant. Le Service doit décider quelle source explorer, et dans quelle mesure. Une fois de plus, après avoir reçu des directives gouvernementales et après avoir établi des lignes directrices sur le partage d'informations avec ses alliés sûrs et avec des organismes soupçonnés de violations des droits de l'homme, le SCRS doit maintenant combler les lacunes procédurales qui se posent lorsque de telles ententes commencent à produire des renseignements. Dans certains cas, le Service a répondu aux attentes, tandis que dans d'autres, le CSARS a constaté que certains des outils spécifiques dont SCRS se sert pour prendre de décisions étaient quelque peu déficients.

INSTITUTIONNALISER LA RESPONSABILITÉ

La nécessité d'établir une chaîne solide et cohérente de responsabilité, dernière « lacune » identifiée quand le CSARS a examiné la redistribution des priorités et des enquêtes, a été notée dans plusieurs études. L'une d'elles, qui porte sur le soutien du SCRS au périmètre de sécurité du Nord du Canada, a souligné combien la question avait évolué au cours des dernières années. En effet se pose la nécessité de trouver un équilibre entre le gouvernement qui souligne le problème de sécurité potentiel que peut poser l'Arctique, et le manque historique de collecte de renseignements dans cette région. En fin de compte, le Comité a constaté que, malgré certaines améliorations, la stratégie pour le Nord du SCRS laissait encore trop au hasard et reposait sur la mobilisation de chefs de file du Service. Sur le long terme, le SCRS, qui devrait adopter une approche centralisée plutôt qu'un leadership régionalisé, devra élaborer une stratégie ciblée, ce qui exige un plan concret, plurianuel, et soutenu par les ressources appropriées.

D'un autre côté, le CSARS a examiné les activités du SCRS liées aux enquêtes au Canada et aux questions émergentes. Au cours des dernières années, les préoccupations nationales de longue date, comme les

accrue entre ces deux mondes est l'érosion potentielle du contrôle sur l'information partagée.

Une plus grande coopération entre les deux organismes est inévitable et souhaitable. Compte tenu de ce fait, le CSARS a identifié un besoin de renforcer de nombreux programmes individuels avec un éventail plus complet de politiques et des procédures, et ce, afin de répondre aux défis croissants qui se posent et à la nécessité de veiller à ce que les deux organismes continuent à respecter leur mandat.

Dans une autre étude sur le nouveau pouvoir octroyé *sur le SCRS*, le CSARS a également constaté que, compte tenu de la nécessité actuelle de tirer parti des partenariats internationaux afin de garder la trace des cibles du SCRS quand elles voyagent à l'étranger, le Service avait entrepris d'optimiser les mécanismes et partenariats existants, et ce, afin d'augmenter sa capacité de collection de renseignements. Cependant, l'augmentation du volume des renseignements résultant du partage de l'information a également entraîné une diminution du niveau de contrôle sur le flux, et

potentiellement l'usage, des renseignements émanant du SCRS, une fois transmis à des partenaires. Bien que le Service ait déjà été identifié ce risque avec l'un de ses alliés, le CSARS a recommandé que le recours à des « mises en garde », c'est à dire à l'annonce explicite des conditions et de limites concernant l'utilisation des renseignements du SCRS, soit appliqué à un plus large éventail de partenariats internationaux.

CONSOLIDER INDICATEURS ET LIMITES

Le CSARS et le SCRS le disent depuis plusieurs années : la lutte contre le terrorisme demeure l'une des plus grandes priorités en matière de renseignement, mais les activités de contre-espionnage sont redevenues un sujet d'actualité. Une telle menace ne s'était pas vue depuis la fin de la guerre froide, et le rôle traditionnel du SCRS, qui consistait à conseiller le gouvernement sur le risque de collecte active de renseignements par d'autres États, a évolué : de simples stratégies et activités « classiques » de contre-espionnage (p.ex. politique et militaire), on est passé à la collecte de renseignements commerciaux et financiers, à la création de réseaux d'influence et, peut-être, plus spectaculairement encore, au morcellement de téraoctets d'informations pour identifier les circonstances et l'origine d'attaques

royale du Canada, le ministre des Affaires étrangères et du Commerce international (MAECI), le ministre de la Défense nationale, l'Agence des services frontaliers du Canada et, en particulier, le Centre de la sécurité des télécommunications Canada (CSTC). En outre, tous les ministères et toutes les agences du gouvernement, et à plus forte raison les proches alliés du Canada, ont de plus en plus recours à la technologie. Les gouvernements des pays occidentaux ont réagi et se sont adaptés, en intégrant d'avantage des organisations de renseignement qui étaient autrefois bien distinctes. Les barrières technologiques cloisonnant les systèmes d'information et les bases de données continuent à tomber, et le partage des données, désormais possible, est devenu monnaie courante. Dans ce rapport annuel, nous examinons les avantages et les risques inhérents à ce changement, et nous mettons en évidence les défis croissants liés à l'examen complet et efficace des activités.

Le SCRS s'apprête à tirer profit de cette nouvelle capacité, mais le CSARS doit aussi être en mesure de réagir. Le Comité doit montrer suffisamment de souplesse pour suivre et examiner efficacement les activités et enquêtes du SCRS, même lorsque celles-ci s'étendent à d'autres agences et ministères. Compte tenu de l'inévitable de l'interconnexion technologique, le CSARS doit avoir en main les outils législatifs et des engagements du gouvernement en matière de ressources pour s'assurer que son rôle de frein et de contrepoids demeure pertinent et efficace.

ETUDES DU CSARS

Cette année, l'intérêt que le Comité manifeste depuis longtemps envers le renforcement de la collaboration entre le SCRS et le Centre de la sécurité des télécommunications Canada (CSTC) nous a conduits à rédiger l'une de nos plus grandes études. Ce partenariat en matière de renseignement devrait être l'un des plus importants des dix prochaines années, et l'étude du CSARS a mis en évidence les grands gains d'efficacité potentiels d'une plus grande coopération en matière de partage des services ou des renseignements, ainsi que les domaines où les résultats étaient encore en deçà des attentes. En matière de partage des renseignements, le CSARS a trouvé des limites à l'application des procédures établies liées au renseignement de source humaine (HUMINT) aux procédures liées au renseignement d'origine électromagnétique (SIGINT). En effet, l'un des grands risques d'une collaboration

BILAN DE
L'EXERCICE

Dans son rapport annuel 2009-2010, le CSARS notait que « les périodes de changements profonds mènent souvent à de graves lacunes en matière de politiques ». Le Comité avait alors demandé au

SCRS et au Parlement d'élaborer une série de questions sur les objectifs et les limites des opérations du Service et de la collecte de renseignements sur la nouvelle grande scène internationale. Dans les années qui suivirent, le Service et le Parlement se sont employés à définir un cadre dans lequel ces objectifs et limites ont été exprimés de façon plus précise, et ce, grâce à la révision des priorités en matière de renseignement, à des lignes directrices plus substantielles sur le partage de l'information, et à des mécanismes pour promouvoir des partenariats canadiens plus efficaces.

Des progrès considérables ont été accomplis pour mieux formuler les priorités et objectifs actuels du SCRS en matière de renseignement. Il est désormais temps de renforcer les règlements et les meilleures pratiques pour assurer d'atteindre ces objectifs, et ce, par l'entremise d'un éventail de mesures appropriées, justifiées et efficaces. Après avoir établi une présence bien plus encadrée et marquée à l'étranger en s'appuyant sur des partenariats canadiens beaucoup plus approfondis et productifs, et après avoir réorganisé ses priorités nationales afin de favoriser de meilleures sources de collecte de renseignements, le SCRS doit revoir plusieurs de ses programmes afin d'identifier leurs objectifs, et de les faire coïncider avec de nouveaux règlements et de nouvelles politiques et procédures opérationnelles.

De même, un changement dans la capacité du CSARS à évaluer pleinement le travail du Service doit venir compléter ces évolutions. En effet, depuis son rapport annuel 2010-2011, le CSARS expose les limites actuelles auquel il se heurte dans l'exercice de son examen, réduit au fonds de renseignements et au personnel du SCRS, et qui est de plus en plus en décalage avec le *modus operandi* du renseignement moderne. Une plus grande coopération avec des partenaires canadiens et des systèmes de partage de l'information plus exhaustifs signifient que les enquêtes du SCRS évoluent au sein d'un réseau de plus en plus étendu. Ce thème se retrouve cette année dans la plupart des études, et il apparaît clairement quand il s'agit de collaboration avec la Gendarmerie

À PROPOS DE CE RAPPORT

Le mandat et les fonctions du CSARS sont définis dans la loi même qui établit le cadre juridique du Service, soit la *Loi sur le Service canadien du renseignement de sécurité*. Conformément à cette loi, le CSARS prépare chaque année un rapport annuel sur ses activités que le ministre de la Sécurité publique transmet au Parlement.

Le présent rapport annuel résume les principales analyses du CSARS, ainsi que les constatations et recommandations qui découlent de ses études et de ses enquêtes sur les plaintes. Il compte trois sections :

SECTION 1

Bilan de l'exercice

Analyse d'importants faits nouveaux dans le domaine du renseignement de sécurité, et de leurs rapports avec certaines constatations et recommandations formulées par le CSARS pendant l'exercice précédent.

SECTION 2

Résumés des études du CSARS

et des plaintes

Résumés des études effectuées par le CSARS et des décisions qu'il a rendues au sujet de plaintes durant la période visée par ce rapport.

SECTION 3

Survol du CSARS

Exposé des activités du CSARS en matière d'intérèssment du public et de liaison et sur le plan administratif. Comprend des détails sur son budget annuel et ses dépenses.

Reportez-vous aux encadrés tout au long du présent rapport annuel. Vous y trouverez de précieux renseignements généraux sur diverses questions juridiques et stratégiques ayant trait aux fonctions de surveillance et d'enquête du CSARS.

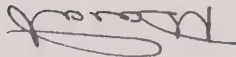
RENSEIGNEMENTS GÉNÉRAUX UTILES ET FACILES À TROUVER

et organismes fédéraux. Cependant, même si la loi ne change pas, je reste convaincu que nos efforts visant à faire évoluer notre travail seront bien reçus par le SCRS et par le Parlement, qui les verront comme un projet constructif.

Dans nos rapports annuels et rapports ministériels sur le rendement ultérieurs, je continuerai à fournir davantage de contexte en termes de progrès réalisés pour faire progresser notre expertise, et ce, afin d'appuyer notre mandat.

Permettez-moi d'affirmer sans équivoque que notre indépendance et notre professionnalisme ne seront jamais mis en péril. Nous sommes déterminées à réaliser notre devoir au nom du Comité, et ce, afin que le Parlement et la population canadienne restent confiants dans l'idée que les services d'espionnage et de renseignement humain du Canada sont pleinement responsables dans l'exercice de leurs fonctions.

Avec toute ma considération,



Michael Doucet

professionnel. Ces échanges permettent également au personnel de tirer parti d'un nombre important et croissant d'experts que nous avons le privilège de consulter au Canada. Enfin, la stratégie essaie également de remédier au risque du phénomène de « pensée de groupe » en assurant que les employés peuvent remplacer les activités du SCRS dans un contexte plus large que celui dans lequel ils travaillent.

En me concentrant sur l'avenir, je garde à l'esprit que l'accès sans entrave du CSARS à l'information du SCRS est notre raison d'être, et que nous pouvons désormais aller encore plus loin avec l'adoption de certaines nouvelles tâches auparavant dévolues à l'ancien Bureau de l'inspecteur général du SCRS. En effet, le Comité est désormais tenu de remettre un certificat au rapport annuel du directeur du SCRS présenté au ministre de la Sécurité publique, indiquant dans quelle mesure il lui paraît acceptable.

Pour nous assurer que l'équipe du Comité peut parfaire sa compréhension professionnelle du SCRS du mieux possible, nos objectifs à court et à moyen terme consistent à intégrer davantage nos trois piliers fondamentaux en termes d'information : les plaintes, les études et la remise du certificat.

Plus généralement, le CSARS continue de jouer un rôle important aux côtés de la communauté du renseignement du Canada, et ce, en contribuant aux débats secrets et publics sur la sécurité nationale. J'envisage d'élargir notre contribution dans ces deux domaines au cours de mon mandat en tant que directeur exécutif du CSARS. Cela prendra du temps, et cela dépendra également de l'élargissement éventuel de la portée légale du CSARS, pour que le Comité puisse suivre le fil d'information sur la sécurité liée au SCRS jusque dans d'autres ministères

ce qui se passe au SCRS, nous devons faire preuve de la plus grande sagesse avec les informations qui nous sont confiées.

Cela dit, afin de rester indépendant du SCRS, le bureau principal du CSARS est situé au centre-ville d'Ottawa. Il s'agit là également d'un « terrain neutre » pour le processus quasi judiciaire d'enquête sur les plaintes, dans le cadre duquel les représentants du SCRS viennent au CSARS pour présenter leur cas. Le CSARS dispose aussi d'un espace de travail au siège du SCRS : c'est là que le personnel du Comité accède aux informations ministérielles et opérationnelles du Service (sur papier et en version électronique), des données qui traitent aussi bien des services de santé que des renseignements bruts sur des opérations très secrètes. Des réunions avec les employés et les gestionnaires du SCRS sont organisées au besoin, et le Comité peut se déplacer dans les bureaux régionaux et les postes à l'étranger du Service. Bref, nous pouvons accéder à tout ce dont nous avons besoin, où que cela se trouve. L'année prochaine, pour la première fois, je me rendrai dans un poste à l'étranger dont l'emplacement est secret. J'irai autant pour l'information que je vais obtenir que pour appuyer le message que ce déplacement souligne : la portée du Comité ne peut être entravée.

Compte tenu de notre accès complet à l'information en matière de sécurité nationale, je reconnais que la confiance accordée à notre travail est ancrée dans la compétence des personnes chargées des activités juridiques et du travail de recherche au nom du Comité.

Cela m'amène à mon deuxième principe : le maintien d'efforts extrêmement compétents et professionnels. Comme on peut s'y attendre, mes employés sont bien formés (à titre d'exemple, les analystes détiennent au moins deux diplômes d'études postsecondaires).

Mon équipe se compose de personnes de différents horizons en termes de formation universitaire et d'expérience professionnelle, et de nombreux employés ont près de dix ans d'expérience ou plus dans la gestion de questions délicates de sécurité nationale. J'ai fait carrière dans les mondes du renseignement et du maintien de l'ordre, et j'ai eu le plaisir de collaborer avec tout un éventail de professionnels canadiens et étrangers dans ces domaines au cours des 25 dernières années. Je peux donc affirmer que je suis impressionné par les évaluations d'experts de l'équipe du CSARS. Des copies de nos rapports classifiés sont transmises au SCRS et au ministre de la Sécurité publique et, par le passé, environ 70 pour cent de nos recommandations ont été acceptées par le Service, même s'il s'agit là de recommandations non exécutoires.

Le troisième principe est complémentaire à la capacité du personnel du CSARS : il s'agit pour le Comité de jouer son rôle de membre productif et informé au sein la communauté de la sécurité nationale. Même si je suis satisfait du travail accompli par mon petit groupe d'experts, je suis tout aussi déterminé à les faire progresser sur le plan professionnel. Ainsi, j'ai entrepris un programme de modernisation qui, grâce à des systèmes technologiques et analytiques supplémentaires, offrira aux employés de nouvelles ressources pour gérer leurs processus juridiques et de recherche.

Je suis également bien conscient qu'améliorer sans cesse les compétences professionnelles de mes employés passe aussi par les initiatives de relations externes du CSARS. Lorsque c'est possible, nous encourageons les employés à établir un lien avec des professionnels issus des milieux universitaire, juridique, du renseignement, de la vérification et policiers. De telles mesures de liaison visent à s'assurer que le personnel du CSARS reste bien informé des questions liées à leur domaine

MESSAGE DU DIRECTEUR EXÉCUTIF

Quand l'honorable Chuck Strahl m'a nommé directeur exécutif du CSARS en décembre 2012, j'ai été frappé de voir à quel point ce Comité, composé de membres du Conseil privé, était peu connu du public. Cela fait bientôt un an que j'occupe mon nouveau rôle, et je pense que je suis désormais bien placé pour faire la lumière sur le travail et les méthodes du CSARS, et expliquer ce que les membres du parlement et la population canadienne peuvent attendre de nous à l'avenir.

Le Comité se compose de Canadiens d'exception, qui puisent dans leurs expériences personnelles et professionnelle pour évaluer l'information qui leur est présentée sur les activités du SCRS. Les membres, qui sont généralement nommés au Comité pour cinq ans, travaillent à temps partiel tout au long de leur mandat. En tant que membres du Conseil privé, ils sont informés des activités du SCRS et consultés par une équipe dévouée d'experts de la sécurité nationale qui travaille à temps plein, ou par l'entremise des audiences de plaintes.

Le président du Comité délègue au directeur exécutif la responsabilité du fonctionnement quotidien du CSARS. En d'autres termes, il m'incombe de trouver les bonnes personnes et de mettre en œuvre les processus et procédures pour m'assurer que le Comité est bien informé. Je suis en outre chargé de veiller à la bonne gestion financière des fonds publics accordés au CSARS.

Permettez-moi de souligner les grands principes, qui, je crois, sont au cœur du travail que mon équipe et moi-même accomplissons au nom du Comité et, par son entremise, pour les parlementaires, et donc toute la population canadienne.

Je suis bien conscient que l'un des risques que comporte ce principe d'indépendance est de se laisser indument influencer par la culture du secret, ou de se laisser piéger par le « cercle magique » décrit par le romancier John le Carré. Le CSARS doit donc toujours concilier le besoin de transparence concernant les activités du SCRS à l'exigence de protéger les renseignements sur la sécurité nationale. Et je vais être très clair là-dessus : nous ne mettrons jamais en péril la sécurité des Canadiens en communiquant des renseignements qui ne serviraient qu'à embellir l'image du Comité et à le présenter comme une entité pertinente et d'actualité. Même si je suis convaincu que nous sommes toujours à l'écoute de

Le plus important principe est notre indépendance.

Les architectes de la *Loi sur le SCRS* ont compris que le CSARS devait être un organisme externe au pouvoir exécutif du gouvernement, et ce, pour veiller à ce que nos conclusions et recommandations ne soient jamais influencées par des considérations bureaucratiques ou politiques. La *Loi sur le SCRS* répond à cette exigence de deux façons complémentaires. Premièrement, les employés du CSARS ne sont pas membres de l'administration publique centrale : le Comité constitue un employeur distinct. Les employés du CSARS conservent leur poste à la discrétion du Comité, ce qui signifie qu'ils ont des obligations à son égard, et non, dans la plupart des cas, envers les institutions gouvernementales. Deuxièmement, les membres du Comité sont nommés comme membres du Conseil privé par le premier ministre du Canada, après consultation avec les autres partis politiques, et ne peuvent être des députés en exercice au Parlement. Cela signifie que, même si les membres ont des profils politiques divers et viennent de toutes les régions du pays, ils siègent au Comité en position de confiance, et que les prédispositions partisanes ne sont pas les bienvenues.

L'honorable
Chuck StrahlL'honorable
Frances LankinL'honorable
Denis LosierL'honorable
Deborah GreyL'honorable
L. Yves Fortier

MEMBRES DU COMITÉ

Enfin, le CSARS demeure résolu à promouvoir et à enrichir le débat critique au Canada sur les objectifs et les limites du renseignement de sécurité, et les

l'environnement plus large de la sécurité et du renseignement. Au Canada, cela se traduira par l'établissement de liens plus forts avec d'autres organisations d'examen et de surveillance, et une consultation accrue avec les experts appropriés en matière de renseignement et de sécurité. Sur le plan international, cela signifiera faire le suivi des liens importants créés lors d'événements comme la conférence internationale des organismes de surveillance du renseignement.

devoirs et fonctions du SCRS en la matière. Comme cela sera reflété dans ce rapport, que nous présentons avec fierté, nous encourageons le SCRS à réaligner et réviser toute une gamme de politiques et d'approches pour soutenir efficacement ses activités d'enquête clés, favorisant ainsi la sécurité et la sûreté continue de la population canadienne, tout en préservant les droits et libertés dont bénéficie le peuple.

et enthousiaste à l'idée de s'appuyer sur les connaissances et le talent de M^{me} Grey et de M. Fortier au cours des années à venir.

Comme nous l'avions prédit dans le rapport annuel 2011-2012, cette année, le Comité a consacré une partie de son temps et de son énergie à s'attaquer à son nouveau défi : guider le CSARS dans l'évolution de ses responsabilités et de son mandat, notamment la tâche de remise du certificat au directeur du SCRS présentée au ministre. Le CSARS s'est avéré parfaitement en mesure de répondre à cette exigence législative. Une relation symbiotique a déjà commencé à s'établir entre la fonction d'examen du Comité et le processus de remise du certificat, où ces deux tâches se nourrissent mutuellement. C'est finalement l'expertise solidement établie du Comité en matière d'élaboration d'études qui a facilité cette transition.

La cohérence de l'approche entre le travail d'étude bien ancré du CSARS et le processus de remise du certificat a également posé la question de savoir comment préserver l'indépendance au cœur du mandat initial du CSARS tout en répondant aux nouvelles exigences législatives. Comme la méthodologie utilisée dans le processus de remise du certificat est assez semblable à l'approche requise pour que le Comité s'acquie de ses autres responsabilités législatives, il n'y a pas de conflit intrinsèque entre la responsabilité du CSARS de faire rapport au Parlement et celle de remettre un certificat au ministre. En effet, les questions soulevées lors de la remise du certificat au rapport du directeur 2011-2012 ont été abordées dans les récentes études du CSARS, et décrites dans son rapport annuel 2011-2012 présenté au Parlement.

A mesure que l'avenir se profile, nous reconnaissons également la nécessité de redynamiser la promotion du CSARS et de son personnel dans le cadre de

qu'hôte, et plus de 100 études et cas de plaintes. Nous souhaitons à M^{me} Pollak une retraite agréable et sereine, et nous la remercions infiniment pour ses années de loyaux services.

Par ailleurs, le Comité voudrait profiter de l'occasion pour remercier Richard Fadden, ancien directeur du SCRS, pour ses années de collaboration et sa cordialité. Au cours des quatre dernières années, M. Fadden a consacré du temps au CSARS, et a eu une attitude ouverte envers le Comité. Nous garderons de bons souvenirs de notre relation professionnelle avec lui. Nous souhaitons à M. Fadden du succès dans son nouveau poste, et nous nous réjouissons de travailler avec son successeur.

Nous nous tournons maintenant vers l'avenir pour souhaiter la bienvenue au nouveau directeur exécutif du CSARS, Michael Doucet. M. Doucet a travaillé au Centre de la sécurité des télécommunications Canada, où il a occupé le poste de dirigeant principal GRC, où il a occupé le poste de dirigeant principal de l'information. Le Comité et son personnel ont d'ores et déjà été impressionnés par l'enthousiasme et le leadership de M. Doucet, et nous attendons avec intérêt de l'innovation et des progrès sous sa direction au cours des prochaines années.

Le CSARS a aussi récemment accueilli Deborah Grey, C.P., O.C., au rang de membre du Comité. M^{me} Grey dispose d'une vaste expérience dans la promotion et la défense de l'intérêt public à l'échelle nationale. En outre, le Comité vient d'accueillir L. Yves Fortier, C.P., C.C., O.Q., c.r., en tant que nouveau membre. M. Fortier, qui possède une longue expérience en tant qu'arbitre international, avocat plaideur, diplomate et directeur de nombreuses sociétés canadiennes, apporte toute une gamme de précieuses compétences au Comité. Il va sans dire que le président est heureux

MESSAGE DES MEMBRES DU COMITÉ

Naturellement, le CSARS évolue, et l'année a été jalonnée d'événements importants : de nouveaux membres se sont joints à notre Comité, qui a produit ses premiers travaux sous la nouvelle présidence de l'honorable Chuck Strahl; notre mandat a été élargi; notamment pour inclure la remise du certificat du CSARS au rapport annuel du directeur du SCRS présenté au ministre de la Sécurité publique; nous avons engagé un nouveau directeur exécutif; premier changement à la direction en 14 ans; et nous nous sommes attelés au défi de réintégrer le CSARS au sein de la grande communauté du renseignement et de la sécurité au Canada.

Nous avons ici le plaisir de présenter neuf résumés des études approfondies effectuées par notre Comité au cours du dernier exercice, ainsi que les résumés des dossiers de plaintes qui ont été réglés dans cette même période.

Dans un tel rapport, il est important de prendre un moment pour reconnaître les personnes qui nous ont aidés à arriver là où nous en sommes aujourd'hui, ainsi que celles et ceux qui nous guideront à l'avenir. Tout d'abord, le Comité voudrait profiter de l'occasion pour exprimer sa plus profonde gratitude envers Susan Pollak, ancienne directrice exécutive du CSARS. Comme le savent tous les membres de la communauté du renseignement et de la sécurité, c'est un euphémisme que d'affirmer que, pendant ses 14 années de leadership, le nom de M^{me} Pollak et celui du CSARS étaient devenus interchangeables. M^{me} Pollak a dirigé le Comité et son personnel dans une période qui a connu cinq présidents, quatre directeurs du SCRS, la vague tumultueuse de changements après le 11 septembre, deux éditions de la conférence internationale des organismes de surveillance du renseignement en tant

Le Comité de surveillance des activités de renseignement de sécurité (CSARS) a été créé pour assurer que les activités liées au renseignement de sécurité au Canada sont menées de façon efficace et appropriée, dans le respect de la loi, et qu'il existe des mécanismes de reddition des comptes suffisants. Au cours de l'année dernière, le Comité a entamé un renouvellement et un remaniement des processus, et ce, pour réaliser ses objectifs clés. Tout au long de ce processus qu'il a encouragé, le Comité est resté fidèle aux devoirs et fonctions du CSARS qui, depuis 1984, joue le rôle de contrepois essentiel aux pouvoirs extraordinaires dont le Parlement a investi le Service canadien du renseignement de sécurité (SCRS). Notre travail, dont les grandes lignes se trouvent dans le rapport annuel présenté au Parlement et, par son entremise, à la population du Canada, démontre notre engagement à fournir aux Canadiens autant de détails que la loi nous permet d'en divulguer.

Les pouvoirs du CSARS découlent de la même loi qui a créé le SCRS et lui a donné son rôle et ses pouvoirs : le SCRS a pour mandat d'enquêter sur les menaces à la sécurité, telles que définies dans la *Loi sur le SCRS*; tandis que le CSARS a pour mandat d'aider à assurer que le Service respecte les droits fondamentaux et les libertés des Canadiens dans l'exercice de ses activités. En tant qu'organisme indépendant qui relève du Parlement, le CSARS s'est engagé à mener ses activités et les conclusions de son travail dans la plus grande transparence possible, tout en s'assurant de respecter les normes les plus strictes en matière d'informations concernant la sécurité nationale. Ces engagements illustrent les valeurs fondamentales du Comité depuis près de 30 ans.

TABLE DES MATIÈRES

2	MESSAGE DES MEMBRES DU COMITÉ.....
5	MESSAGE DU DIRECTEUR EXÉCUTIF.....
8	À PROPOS DE CE RAPPORT
9	BILAN DE L'EXERCICE.....
14	RÉSUMÉS DES ÉTUDES DU SCRS ET DES PLAINTES.....
14	A. ÉTUDES
16	Les relations et échanges du SCRS avec le Centre de la sécurité des télécommunications Canada (CSTC)
18	Examen du nouveau pouvoir octroyé au moyen de mandat en vertu de l'article 21
19	Le travail d'enquête liée à l'espionnage et à l'influence étrangère
21	Les initiatives du SCRS en matière de collecte à l'étranger
22	L'évolution de la marque du SCRS à l'étranger
23	L'appui du SCRS au périmètre de sécurité du Nord du Canada
25	Les activités du SCRS liées aux enquêtes nationales et aux questions émergentes
26	Le recours du SCRS aux méthodes clandestines
27	Le rôle du SCRS dans l'affaire Abdelrazik
31	Remise du certificat au rapport annuel du directeur du SCRS au ministre de la sécurité publique : survol.....
33	B. PLAINTES.....
35	Allégations de harcèlement, de profilage racial et de partage de données trompeuses
35	Allégations de refus des droits fondamentaux et de connaissances culturelles insuffisantes de la part du SCRS
36	Allégations de retard à fournir une évaluation de sécurité
36	Révocation d'habilitations de sécurité
37	SURVOL DU SCRS.....
37	Composition du comité.....
37	Personnel et organisation
38	Activités du comité
39	Liste des recommandations du CSARS



À PROPOS DU CSARS

Le Comité de surveillance des activités de renseignement de sécurité (CSARS ou Comité) est un organisme indépendant qui rend compte des opérations du Service canadien du renseignement de sécurité (SCRS ou Service) au Parlement du Canada. Le CSARS effectue des études sur les activités du SCRS et enquête sur les plaintes du public contre le Service. Cela lui permet de fournir au Parlement, et à tous les citoyens du Canada, l'assurance que le Service enquête sur les menaces à la sécurité nationale et fait rapport à ce sujet d'une façon qui respecte la primauté du droit et les droits des Canadiens.

Pour plus de renseignements sur le CSARS, veuillez consulter le site www.sirc-csars.gc.ca.

À PROPOS DU SCRS

Le SCRS a la responsabilité d'enquêter sur les menaces contre le Canada, d'analyser l'information et de produire des renseignements. Pour protéger le Canada et ses citoyens, le SCRS conseille le gouvernement fédéral au sujet des questions et activités qui menacent ou peuvent menacer la sécurité nationale, notamment le terrorisme, la prolifération et armes de destruction massive, l'espionnage et les activités d'insurrection étrangère. Le SCRS fournit également des évaluations de sécurité individuelles pour le compte de tous les ministères et organismes fédéraux, sauf la Gendarmerie royale du Canada.

Cadre juridique du CSARS et du SCRS

Suite à l'adoption de la *Loi sur le SCRS*, le Canada est devenu l'un des premiers pays démocratiques du monde à doter son service de sécurité d'un cadre juridique. Cette *Loi* a clairement défini le mandat et les limites du pouvoir de l'État en matière de renseignement de sécurité. Par ailleurs, elle a créé des mécanismes de reddition de comptes qui permettent de contrôler ce pouvoir considérable.



Le 30 septembre 2013

L'honorable Steven Blaney
Ministre de la Sécurité publique
Chambre des communes
Ottawa (Ontario)
K1A 0A6

Monsieur le Ministre,

C'est pour nous un plaisir de vous remettre le rapport annuel du Comité de surveillance des activités de renseignement de sécurité pour l'exercice 2012-2013, tel qu'il est prescrit à l'article 53 de la *Loi sur le Service canadien du renseignement de sécurité*, afin qu'il soit transmis au Parlement.

Veuillez agréer, Monsieur le Ministre, l'expression de notre haute considération.

Chuck Strahl, C.P.
Président

Denis Losier, C.P., C.M.

Frances Lankin, C.P., C.M.

L. Yves Fortier, C.P., C.C., O.Q., c.r.

Deborah Grey, C.P., O.C.

Comité de surveillance des activités de renseignement de sécurité
B.P. 2430, succursale D
Ottawa (Ontario) K1P 5W5

Veuillez consulter notre site Web à www.sirc-csars.gc.ca.

© Travaux publics et Services gouvernementaux Canada 2013
Numéro de catalogue PS 105-2013
ISSN 1921-0566



RAPPORT ANNUEL 2012-2013

Réviser le fonctionnement des activités
de renseignements et de leur surveillance

COMBLER LES LACUNES